Fundusze Europejskie na Rozwój Cyfrowy

ZAŁĄCZNIK I.3

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. Tytuł

Zakup serwerów w ramach realizacji Projektu „Cyberbezpieczny Samorząd”

2. Zamawiający

Urząd Miasta Zielona Góra

Adres: ul. Podgórna 22
65-213 Zielona Góra

3. Termin wykonania Przedmiotu Zamówienia

Przedmiot Umowy musi być zrealizowany terminie: 20 dni kalendarzowych od dnia zawarcia Umowy. Adres Zamawiającego jest też właściwym dla miejsca dostawy dostarczanych urządzeń.

4. Przedmiot Zamówienia i wymagania ogólne

4.1. Dostawa serwerów obejmuje dostawę maszyn fizycznych zgodnych ze specyfikacją oraz wyspecyfikowanego oprogramowania serwerowego niezbędnego do ich eksploatacji.

4.2. Przedmiot zamówienia musi być legalny, fabrycznie nowy, nigdy wcześniej nie używany, pochodzący z legalnego kanału dystrybucyjnego, dopuszczony do obrotu, spełniający normy CE. Nie dopuszcza się urządzeń typu refurbished (zwróconych do producenta i później odsprzedawanych ponownie przez producenta).

4.3. Zamawiający wymaga, aby wszystkie dostarczane urządzenia i pakiety oprogramowania były sprawdzone w praktyce rynkowej. Oznacza to, iż oprogramowanie systemowe (firmware urządzeń) realizujące wszystkie wymagane funkcje jak też samo urządzenie musiało być dostępne na rynku co najmniej 6 miesięcy przed terminem składania ofert.

4.4. Urządzenie i powiązane z nim oprogramowanie systemowe musi być objęte pełnym serwisem producenta (niedopuszczalne jest proponowanie oprogramowanie np. w wersji Beta) w chwili, i co najmniej w okresie 6 miesięcy przed złożeniem ofert. Za datę jego dostępności Zamawiający przyjmuje publikację konkretnej oferowanej wersji oprogramowania (wersji z pełnym wsparciem) na stronie Producenta rozwiązania

4.5. Zadanie uznane zostanie przez Zamawiającego, gdy Wykonawca wykona opisane poniżej czynności co zostanie potwierdzone przez Zamawiającego poprzez podpisanie Odbioru Protokołu Odbioru Końcowego bez zastrzeżeń.

5. Serwer wirtualizacyjny typ 1

5.1	Obudowa: 1. Obudowa Rack o wysokości max 2U . 2. 8 wnęk na dyski 2.5”.

Departament Organizacyjny - Biuro Zamówień Publicznych www.zielona-gora.pl
ul. Stary Rynek 13, 65-067 Zielona Góra e-mail: zamowienia@um.zielona-gora.pl
tel. (+48) 68 45 64 419

	3. 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.
5.2	Płyta główna: 1. Płyta główna z możliwością zainstalowania do dwóch procesorów. 2. Obsługa procesorów 144 rdzeniowych. 3. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. 4. Na płycie głównej powinno znajdować się minimum 24 sloty przeznaczone do instalacji pamięci. 5. Płyta główna powinna obsługiwać do 6TB pamięci RAM.
5.3	Procesor: 1. Zainstalowane dwa procesory min. 16-rdzeniowe, min. 3.2GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 252 w teście SPECspeed®2017_fp_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej oferowanego serwera.
5.4	Pamięć RAM: 1. 512GB DDR5 RDIMM 6400MT/s.
5.5	Kontroler RAID: 1. Sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID: 0, 1, 10 (obsługa dysków NVMe)
5.6	Dyski twarde: 1. Zainstalowane: 1.a. 1x dysk NVMe o pojemności min. 6.4TB do mieszanych zastosowań, Hot-Plug 2. Zainstalowane 2x dysk M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
5.7	Gniazda PCI: 1. Cztery sloty PCIe. 2. Dwa sloty OCP.
5.8	Interfejsy sieciowe: 1. 1x czteroportowa karta sieciowa 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe). 2. 2x dwuportowa karta sieciowa 25Gb Ethernet w standardzie SFP28. 3. 8x wkładka 25GbE SFP28 SR.
5.9	Wbudowane porty: 1. 4 porty USB w tym min: 1.1 1x port USB 2.0 Type-C. 1.2 2x porty USB 3.1. 1.3 1x port USB 3.0 wewnątrz obudowy. 2. Port VGA z tyłu obudowy.
5.10	Video: 1. Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200.
5.11	Zasilacze:

Departament Organizacyjny - Biuro Zamówień Publicznych www.zielona-gora.pl
ul. Stary Rynek 13, 65-067 Zielona Góra e-mail: zamowienia@um.zielona-gora.pl
tel. (+48) 68 45 64 419

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Cyberbezpieczny Samorząd

	1. Redundantne, Hot-Plug min. 1500W klasy Titanium
5.12	Elementy montażowe: 1. Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. 2. Uchwyt do trzymania kabli
5.13	Bezpieczeństwo: 1. Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. 2. 2. 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. 3. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. 4. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła. 5. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. 6. Moduł TPM 2.0. 7. Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera. 8. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem. 9. 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).
5.14	Karta zarządzania: Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca: 1. zdalny dostęp do graficznego interfejsu Web karty zarządzającej. 2. szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika. 3. możliwość podmontowania zdalnych wirtualnych napędów. 4. wirtualną konsolę z dostępem do myszy, klawiatury. 5. wsparcie dla IPv6. 6. wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH. 7. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer 8. możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer. 9. integracja z Active Directory. 10. możliwość obsługi przez sześciu administratorów jednocześnie. 11. Wsparcie dla automatycznej rejestracji DNS. 12. wsparcie dla LLDP. 13. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. 14. możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy. 15. Monitorowanie zużycia dysków SSD.

Departament Organizacyjny - Biuro Zamówień Publicznych www.zielona-gora.pl
ul. Stary Rynek 13, 65-067 Zielona Góra e-mail: zamowienia@um.zielona-gora.pl
tel. (+48) 68 45 64 419

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Cyberbezpieczny Samorząd

	16. Automatyczne zgłaszanie alertów do centrum serwisowego producenta. 17. Automatyczne update firmware dla wszystkich komponentów serwera. 18. Możliwość przywrócenia poprzednich wersji firmware. 19. Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON. 20. Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych. 21. Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram. 22. Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera. 23. kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania. 24. możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień. 25. możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera. 26. możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer. 27. możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe. Możliwość rozszerzenia funkcjonalności o: 1. 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. 2. możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej. 3. Automatyczne odświeżanie certyfikatów SSL. 4. monitorowanie przepływu powietrza na bieżąco (w CFM).
5.15	Oprogramowanie do zarządzania: Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: 1. Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych 2. integracja z Active Directory 3. Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta 4. Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish 5. Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram 6. Szczegółowy opis wykrytych systemów oraz ich komponentów 7. Możliwość eksportu raportu do CSV, HTML, XLS, PDF 8. Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. 9. Grupowanie urządzeń w oparciu o kryteria użytkownika 10. Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji 11. Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach 12. Szybki podgląd stanu środowiska 13. Podsumowanie stanu dla każdego urządzenia 14. Szczegółowy status urządzenia/elementu/komponentu

Departament Organizacyjny - Biuro Zamówień Publicznych
ul. Stary Rynek 13, 65-067 Zielona Góra
tel. (+48) 68 45 64 419
www.zielona-gora.pl
e-mail: zamowienia@um.zielona-gora.pl

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Cyberbezpieczny Samorząd

	15. Generowanie alertów przy zmianie stanu urządzenia. 16. Filtry raportów umożliwiające podgląd najważniejszych zdarzeń 17. Integracja z service desk producenta dostarczonej platformy sprzętowej 18. Możliwość przejęcia zdalnego pulpitu 19. Możliwość podmontowania wirtualnego napędu 20. Kreator umożliwiający dostosowanie akcji dla wybranych alertów 21. Możliwość importu plików MIB 22. Przesyłanie alertów „as-is" do innych konsol firm trzecich 23. Możliwość definiowania ról administratorów 24. Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów 25. Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) 26. Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta 27. Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów 28. 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. 29. Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. 30. Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile 31. Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. 32. Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. 33. Zdalne uruchamianie diagnostyki serwera. 34. Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. 35. Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. 36. Integracja z środowiskiem VMware vCenter pozwalająca z konsoli/plugin: 37. wykonać zautomatyzowaną aktualizację firmware serwerów w klastrze Vmware do zdefiniowanej polityki poziomu mikrokodów 37.1. wykonać/zweryfikować konfigurację serwera zgodną ze zdefiniowaną polityka konfiguracji 37.2. z konsoli vCenter uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny) 37.3. inwentaryzacja komponentów w serwerze i ich mikrokodów 37.4. historia poboru mocy i temperatury serwera 37.5. zbieranie danych diagnostycznych serwera do paczki serwisowej
5.16	Oprogramowanie do monitorowania: Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:

Departament Organizacyjny - Biuro Zamówień Publicznych
ul. Stary Rynek 13, 65-067 Zielona Góra
tel. (+48) 68 45 64 419
www.zielona-gora.pl
e-mail: zamowienia@um.zielona-gora.pl

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Cyberbezpieczny Samorząd

	1. Monitoring: 1.a. ilość podłączonych oraz rozłączonych systemów 1.b. stan podłączonych urządzeń 1.c. informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów 1.d. Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia 1.e. informacje o statusie gwarancji dla poszczególnych urządzeń 1.f. informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń 1.g. informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. 1.h. Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych 1.i. 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. 1.j. Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. 1.k. Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. 1.l. Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. 1.m. 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. 1.n. 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 1.o. Monitoring parametrów przełączników sieciowych z informacją o minimum: ▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny

Departament Organizacyjny - Biuro Zamówień Publicznych www.zielona-gora.pl
ul. Stary Rynek 13, 65-067 Zielona Góra e-mail: zamowienia@um.zielona-gora.pl
tel. (+48) 68 45 64 419

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Cyberbezpieczny Samorząd

	▪ 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. 2. Aktualizacja firmware 2.a. możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania 2.b. możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania 2.c. możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania 2.d. możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania 2.e. możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania 3. Raporty 3.a. 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, 3.b. 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 3.c. Generowanie raportów do plików CSV i PDF 4. Cyberbezpieczeństwo 4.a. 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. 4.b. Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. 4.c. Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. 4.d. Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. 5. Wspierane urządzenia 5.a. Urządzenie Producenta dostarczane w ramach postępowania 5.b. Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) 6. Wirtualny asystent

Departament Organizacyjny - Biuro Zamówień Publicznych www.zielona-gora.pl
ul. Stary Rynek 13, 65-067 Zielona Góra e-mail: zamowienia@um.zielona-gora.pl
tel. (+48) 68 45 64 419

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Cyberbezpieczny Samorząd

	6.a. 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; 7. Możliwość rozszerzenia funkcjonalności 7.a. Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. 8. Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android
5.17	Certyfikaty: 1. Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 2. Serwer musi posiadać deklaracja CE. 3. Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver, dla kraju, w którym produkt będzie użytkowany, według normy wprowadzonej w 2019 roku – dokumenty potwierdzające należy załączyć do oferty. 4. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025.
5.18	Dokumentacja użytkownika: 1. Zamawiający wymaga dokumentacji w języku polskim lub angielskim. 2. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
5.19	Warunki gwarancji: 1. Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. 2. Możliwość bezpłatnego pobierania aktualizacji firmware, BIOS i sterowników po wygaśnięciu gwarancji. 3. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet. 4. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) 5. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.

Departament Organizacyjny - Biuro Zamówień Publicznych www.zielona-gora.pl
ul. Stary Rynek 13, 65-067 Zielona Góra e-mail: zamowienia@um.zielona-gora.pl
tel. (+48) 68 45 64 419

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Cyberbezpieczny Samorząd

	6. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon/portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. 7. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. 8. 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. 9. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. 10. 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. 11. 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. 12. Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: 12.1. Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. 12.2. 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. 12.3. Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. 12.4. 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. 12.5. 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. 13. 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. 14. Ze względu na bezpieczeństwo danych Wykonawca musi posiadać certyfikat ISO- 27001 na projektowanie, sprzedaż i wdrażanie rozwiązań teleinformatycznych – dokumenty potwierdzające należy załączyć do oferty.

Departament Organizacyjny - Biuro Zamówień Publicznych
ul. Stary Rynek 13, 65-067 Zielona Góra
tel. (+48) 68 45 64 419
www.zielona-gora.pl
e-mail: zamowienia@um.zielona-gora.pl

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Cyberbezpieczny Samorząd

5.20	Ilość sztuk dostarczanego sprzętu: Należy dostarczyć 1 urządzenie wedle wskazanej specyfikacji.

Departament Organizacyjny - Biuro Zamówień Publicznych
ul. Stary Rynek 13, 65-067 Zielona Góra
tel. (+48) 68 45 64 419
www.zielona-gora.pl
e-mail: zamowienia@um.zielona-gora.pl

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Cyberbezpieczny Samorząd

6. Serwer wirtualizacyjny typ 2

6.1	Obudowa: 1. Obudowa Rack o wysokości max 2U . 2. 8 wnęk na dyski 2.5”. 3. 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.
6.2	Płyta główna: 1. Płyta główna z możliwością zainstalowania do dwóch procesorów. 2. Obsługa procesorów 144 rdzeniowych. 3. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. 4. Na płycie głównej powinno znajdować się minimum 24 sloty przeznaczone do instalacji pamięci. 5. Płyta główna powinna obsługiwać do 6TB pamięci RAM.
6.3	Procesor: 1. Zainstalowane dwa procesory min. 16-rdzeniowe, min. 3.2GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 252 w teście SPECspeed®2017_fp_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej oferowanego serwera.
6.4	Pamięć RAM: 1. 512GB DDR5 RDIMM 6400MT/s.
6.5	Kontroler RAID: 2. Sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID: 0, 1, 10 (obsługa dysków NVMe)
6.6	Dyski twarde: 1. Zainstalowane: 1.1 1x dysk NVMe o pojemności min. 1.6TB do mieszanych zastosowań, Hot-Plug 2. Zainstalowane 2x dysk M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
6.7	Gniazda PCI: 1. Cztery sloty PCIe. 2. Dwa sloty OCP.
6.8	Interfejsy sieciowe: 1. 1x czteroportowa karta sieciowa 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe). 2. 2x dwuportowa karta sieciowa 25Gb Ethernet w standardzie SFP28. 3. 8x wkładka 25GbE SFP28 SR.
6.9	Wbudowane porty: 1. 4 porty USB w tym min: 1.1 1x port USB 2.0 Type-C. 1.2 2x porty USB 3.1.

Departament Organizacyjny - Biuro Zamówień Publicznych www.zielona-gora.pl
ul. Stary Rynek 13, 65-067 Zielona Góra e-mail: zamowienia@um.zielona-gora.pl
tel. (+48) 68 45 64 419

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Cyberbezpieczny Samorząd

	1.3 1x port USB 3.0 wewnątrz obudowy. 2. Port VGA z tyłu obudowy.
6.10	Video: 1. Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200.
6.11	Zasilacze: 1. Redundantne, Hot-Plug min. 1500W klasy Titanium
6.12	Elementy montażowe: 1. Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. 2. Uchwyt do trzymania kabli.
6.13	Bezpieczeństwo: 1. Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. 2. 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. 3. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. 4. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła. 5. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. 6. Moduł TPM 2.0. 7. Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera. 8. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem. 9. 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).
6.14	Karta zarządzania: Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca: 1. zdalny dostęp do graficznego interfejsu Web karty zarządzającej. 2. szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika. 3. możliwość podmontowania zdalnych wirtualnych napędów. 4. wirtualną konsolę z dostępem do myszy, klawiatury. 5. wsparcie dla IPv6. 6. wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH. 7. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer 8. możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer. 9. integracja z Active Directory. 10. możliwość obsługi przez sześciu administratorów jednocześnie. 11. Wsparcie dla automatycznej rejestracji DNS. 12. wsparcie dla LLDP.

Departament Organizacyjny - Biuro Zamówień Publicznych www.zielona-gora.pl
ul. Stary Rynek 13, 65-067 Zielona Góra e-mail: zamowienia@um.zielona-gora.pl
tel. (+48) 68 45 64 419

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Cyberbezpieczny Samorząd

	13. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. 14. możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy. 15. Monitorowanie zużycia dysków SSD. 16. Automatyczne zgłaszanie alertów do centrum serwisowego producenta. 17. Automatyczne update firmware dla wszystkich komponentów serwera. 18. Możliwość przywrócenia poprzednich wersji firmware. 19. Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON. 20. Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych. 21. Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram. 22. Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera. 23. kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania. 24. możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień. 25. możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera. 26. możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer. 27. możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe. Możliwość rozszerzenia funkcjonalności o: 5. 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. 6. możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej. 7. Automatyczne odświeżanie certyfikatów SSL. 8. monitorowanie przepływu powietrza na bieżąco (w CFM).
6.15	Oprogramowanie do zarządzania: Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: 1. Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych 2. integracja z Active Directory 3. Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta 4. Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish 5. Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram 6. Szczegółowy opis wykrytych systemów oraz ich komponentów 7. Możliwość eksportu raportu do CSV, HTML, XLS, PDF 8. Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. 9. Grupowanie urządzeń w oparciu o kryteria użytkownika

Departament Organizacyjny - Biuro Zamówień Publicznych
ul. Stary Rynek 13, 65-067 Zielona Góra
tel. (+48) 68 45 64 419
www.zielona-gora.pl
e-mail: zamowienia@um.zielona-gora.pl

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Cyberbezpieczny Samorząd

	10. Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji 11. Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach 12. Szybki podgląd stanu środowiska 13. Podsumowanie stanu dla każdego urządzenia 14. Szczegółowy status urządzenia/elementu/komponentu 15. Generowanie alertów przy zmianie stanu urządzenia. 16. Filtry raportów umożliwiające podgląd najważniejszych zdarzeń 17. Integracja z service desk producenta dostarczonej platformy sprzętowej 18. Możliwość przejęcia zdalnego pulpitu 19. Możliwość podmontowania wirtualnego napędu 20. Kreator umożliwiający dostosowanie akcji dla wybranych alertów 21. Możliwość importu plików MIB 22. Przesyłanie alertów „as-is" do innych konsol firm trzecich 23. Możliwość definiowania ról administratorów 24. Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów 25. Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) 26. Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta 27. Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów 28. 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. 29. Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. 30. Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile 31. Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. 32. Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. 33. Zdalne uruchamianie diagnostyki serwera. 34. Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. 35. Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. 36. Integracja z środowiskiem VMware vCenter pozwalająca z konsoli/plugin: 37. wykonać zautomatyzowaną aktualizację firmware serwerów w klastrze Vmware do zdefiniowanej polityki poziomu mikrokodów 37.1. wykonać/zweryfikować konfigurację serwera zgodną ze zdefiniowaną polityka konfiguracji 37.2. z konsoli vCenter uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny) 37.3. inwentaryzacja komponentów w serwerze i ich mikrokodów

Departament Organizacyjny - Biuro Zamówień Publicznych
ul. Stary Rynek 13, 65-067 Zielona Góra
tel. (+48) 68 45 64 419
www.zielona-gora.pl
e-mail: zamowienia@um.zielona-gora.pl

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Cyberbezpieczny Samorząd

	37.4. historia poboru mocy i temperatury serwera 37.5. zbieranie danych diagnostycznych serwera do paczki serwisowej
6.16	Oprogramowanie do monitorowania: Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: 1. Monitoring: 1.1 ilość podłączonych oraz rozłączonych systemów 1.2 stan podłączonych urządzeń 1.3 informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów 1.4 Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia 1.5 informacje o statusie gwarancji dla poszczególnych urządzeń 1.6 informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń 1.7 informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. 1.8 Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych 1.9 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. 1.10 Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. 1.11 Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. 1.12 Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. 1.13 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.

Departament Organizacyjny - Biuro Zamówień Publicznych www.zielona-gora.pl
ul. Stary Rynek 13, 65-067 Zielona Góra e-mail: zamowienia@um.zielona-gora.pl
tel. (+48) 68 45 64 419

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Cyberbezpieczny Samorząd

	▪ 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 1.14 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. 2. Aktualizacja firmware 2.1 możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania 2.2 możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania 2.3 możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania 2.4 możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania 2.5 możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania 3. Raporty 3.1 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, 3.2 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 3.3 Generowanie raportów do plików CSV i PDF 4. Cyberbezpieczeństwo 4.1 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. 4.2 Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. 4.3 Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.

Departament Organizacyjny - Biuro Zamówień Publicznych www.zielona-gora.pl
ul. Stary Rynek 13, 65-067 Zielona Góra e-mail: zamowienia@um.zielona-gora.pl
tel. (+48) 68 45 64 419

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Cyberbezpieczny Samorząd

	4.4 Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. 5. Wspierane urządzenia 5.1 Urządzenie Producenta dostarczane w ramach postępowania 5.2 Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) 6. Wirtualny asystent 6.1 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; 7. Możliwość rozszerzenia funkcjonalności 7.1 Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. 8. Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android
6.17	Certyfikaty: 1. Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 2. Serwer musi posiadać deklaracja CE. 3. Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver, dla kraju, w którym produkt będzie użytkowany, według normy wprowadzonej w 2019 roku – dokumenty potwierdzające należy załączyć do oferty. 4. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025.
6.18	Dokumentacja użytkownika: 1. Zamawiający wymaga dokumentacji w języku polskim lub angielskim. 2. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
6.19	Warunki gwarancji: 1. Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. 2. Możliwość bezpłatnego pobierania aktualizacji firmware, BIOS i sterowników po wygaśnięciu gwarancji. 3. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet.

Departament Organizacyjny - Biuro Zamówień Publicznych www.zielona-gora.pl
ul. Stary Rynek 13, 65-067 Zielona Góra e-mail: zamowienia@um.zielona-gora.pl
tel. (+48) 68 45 64 419

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Cyberbezpieczny Samorząd

	4. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) 5. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. 6. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon/portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. 7. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. 8. 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. 9. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. 10. 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. 11. 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. 12. Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: 12.1. Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. 12.2. 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. 12.3. Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. 12.4. 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. 12.5. 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.

Departament Organizacyjny - Biuro Zamówień Publicznych
ul. Stary Rynek 13, 65-067 Zielona Góra
tel. (+48) 68 45 64 419
www.zielona-gora.pl
e-mail: zamowienia@um.zielona-gora.pl

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Cyberbezpieczny Samorząd

	13. 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. 14. Ze względu na bezpieczeństwo danych Wykonawca musi posiadać certyfikat ISO- 27001 na projektowanie, sprzedaż i wdrażanie rozwiązań teleinformatycznych – dokumenty potwierdzające należy załączyć do oferty.
6.20	Ilość sztuk dostarczanego sprzętu: Należy dostarczyć 2 urządzenie wedle wskazanej specyfikacji.
7	Wymagania dodatkowe: a) Wszystkie wymagania dodatkowe będą weryfikowane tylko w przypadku ofert, które po weryfikacji ze strony Zamawiającego spełniły podstawowe wymagania określone w punkcie 5 i 6 Specyfikacji tj. Serwer wirtualizacyjny typ 1 oraz Serwer wirtualizacyjny typ 2. b) Łącznie Zamawiający przyzna od 0 do 25 punktów za spełnienie ww. wymagań dodatkowych
7.1	Chmurowa platforma producenta do proaktywnego monitoringu z wykrywaniem anomalii (ML) i wbudowanym asystentem GenAI © 1. Proaktywny monitoring stanu urządzeń w chmurze; 2. Wykrywanie anomalii wydajnościowych oparte o uczenie maszynowe. Potwierdzenie funkcjonalności na podstawie zapisów w dokumentacji i/lub wydruku z portalu producenta serwera potwierdzającego dostępność wszystkich wyszczególnionych funkcjonalności. Zamawiający przyzna dodatkowe 20 punktów, jeżeli dostarczone serwery będą oferowały ww. funkcjonalności lub 0 punktów, jeśli nie będą oferowały niniejszej usługi.
7.2	Funkcje bezpieczeństwa i zarządzania 1. Aktualizacja firmware kontrolera zarządzającego, nośników NVMe i kontrolera RAID bez restartu serwera. 2. Udostępnianie SBOM oprogramowania układowego (CycloneDX/SPDX). 3. Licencja karty zarządzającej w najwyższym poziomie, bezterminowa. Potwierdzenie funkcjonalności na podstawie zapisów w dokumentacji lub wydruku z portalu producenta serwera potwierdzającego dostępność wszystkich wyszczególnionych funkcjonalności lub w szczególnych przypadkach w oparciu o oświadczenie producenta urządzenia. Zamawiający przyzna dodatkowe 5 punktów, jeżeli dostarczone serwery będą oferowały ww. funkcjonalność lub 0 punktów, jeśli nie będą oferowały wskazanych funkcji.

Departament Organizacyjny - Biuro Zamówień Publicznych
ul. Stary Rynek 13, 65-067 Zielona Góra
tel. (+48) 68 45 64 419
www.zielona-gora.pl
e-mail: zamowienia@um.zielona-gora.pl

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Cyberbezpieczny Samorząd