Miejscowość: \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Data: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Załącznik nr 1**

**FORMULARZ OFERTOWY**

**ZAPYTANIE OFERTOWE nr 28/** **Serwery wraz z licencją na oprogramowanie**

Nazwa Wykonawcy:

Adres:

NIP:

Nr telefonu:

Adres e-mail:

Dane osoby do kontaktu:

W odpowiedzi na zapytanie ofertowe pn. *ZAPYTANIE OFERTOWE nr 28/ Serwery wraz z licencją na oprogramowanie* oferuję wykonanie przedmiotu zamówienia, zgodnie z wymogami i zakresem określonym w zapytaniu ofertowym, za:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Przedmiot zamówienia** | **Waluta oferty****(PLN / EUR)** | **Ogółem wartość NETTO we wskazanej walucie** | **Wartość podatku VAT we wskazanej walucie** | **Ogółem wartość BRUTTO we wskazanej walucie** |
| Serwery wraz z licencją na oprogramowanie |  |  |  |  |

**Całkowita wartość zamówienia brutto słownie:**

1. **Ceny wskazane w tabeli uwzględniają wszystkie koszty związane z wykonaniem przedmiotu zamówienia i są cenami stałymi w okresie obowiązywania umowy.**
2. Cały przedmiot zamówienia będzie posiadał aktualne atesty i certyfikaty bezpieczeństwa poświadczające zgodność z normami obowiązującymi w Unii Europejskiej oraz zgodności i certyfikaty określone w zapytaniu ofertowym.
3. Zobowiązujemy się do wykonania przedmiotu zamówienia z zastosowaniem następujących urządzeń i materiałów:

(***W każdym wierszu tabeli należy podać informację czy/jak oferowany sprzęt spełnia wymagania Zamawiającego. Dopuszcza się wypełnienie wierszy w formule TAK/NIE. W przypadku braku zamieszczenia informacji (braku wypełnienia) w którymkolwiek z obowiązkowych pól, oferta zostanie odrzucona. Wykonawca tam gdzie jest to możliwe wskazuje również „Typ/model oferowanego urządzenia” oraz „Producenta”).***

|  |  |
| --- | --- |
| **Parametry techniczne przedmiotu zamówienia** | **Potwierdzenie spełnienia /****Parametry oferowane[[1]](#footnote-2)** |

|  |  |  |
| --- | --- | --- |
| **Urządzenie typu 1 – serwer – 2 sztuki** | **Obudowa*** Obudowa Rack o wysokości nie większej niż 1U z możliwością instalacji do 8 dysków 2.5" Hot- Plug
* Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze.
 |  |
| **Płyta główna****•** Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.• Na płycie głównej musi znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci RAM o sumarycznej pojemności do 1TB |  |
| **Procesor** * Zainstalowane dwa procesory 12-rdzeniowe, min. 3GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 195 w teście

SPECrate2017\_int\_base dostępnym na stronie www.spec.org dla dwóch procesorów. |  |
| **RAM**  512 GB DDR4 RDIMM 3200MT/s lub lepsze |  |
| **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 |  |
| **Dyski twarde** Zainstalowane: 2x dysk SATA SSD o pojemności min. 480GB, Hot-Plug. |  |
| **Interfejsy sieciowe/ SAS** • Wbudowana dwuportowa karta sieciowa posiadająca co najmniej dwa porty 1Gb BaseT* dwuportowa karta sieciowa typu OCP w wersji 3.0, posiadająca co najmniej dwa porty SFP28, wspierająca prędkości 10Gb oraz 25Gb

• dwuportowa karta sieciowa PCIe, posiadająca co najmniej dwa porty SFP28, wspierająca prędkości 10Gb oraz 25Gb |  |
| **Wbudowane porty** * Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej,

 • Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0 |  |
| **Wideo** Zintegrowana karta graficzna umożliwiająca wyświetlenie obrazu o rozdzielczości min. 1600x900 |  |
| **Wentylatory** **•** Redundantne |  |
| **Zasilacze** Redundantne, Hot-Plug minimalnie 1100W klasy Titanium |  |
| **Elementy montażowe** Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych |  |
| **System operacyjny/dodatkowe oprogramowanie****•** Windows Server 2022 Datacenter licencja dla 24 rdzeni, wersja polska lub równoważny |  |
| **Bezpieczeństwo*** Zatrzask górnej pokrywy oraz blokada na ramce panelu 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 wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem |  |
| **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 SSL
* 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;
* integracja z Active Directory;
* 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
* możliwość obsługi przez sześciu użytkowników jednocześnie;
* możliwość podmontowania zdalnych wirtualnych napędów;
* wirtualną konsolę z dostępem do myszy, klawiatury;
* możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; oraz z możliwością rozszerzenia funkcjonalności o: o Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej o Przesyłanie danych telemetrycznych w czasie rzeczywistym

Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze  o Automatyczna rejestracja certyfikatów (ACE) |  |
| **Oprogramowanie do zarządzania**Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: o Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych o integracja z Active Directory o Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta o Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish o Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram o Szczegółowy opis wykrytych systemów oraz ich komponentów o Możliwość eksportu raportu do CSV, HTML, XLS, PDF o Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. o Grupowanie urządzeń w oparciu o kryteria użytkownika o Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji o Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach o Szybki podgląd stanu środowiska o Podsumowanie stanu dla każdego urządzenia o Szczegółowy status urządzenia/elementu/komponentu o Generowanie alertów przy zmianie stanu urządzenia. o Filtry raportów umożliwiające podgląd najważniejszych zdarzeń o Integracja z service desk producenta dostarczonej platformy sprzętowej o Możliwość przejęcia zdalnego pulpitu o Możliwość podmontowania wirtualnego napędu o Kreator umożliwiający dostosowanie akcji dla wybranych alertów o Możliwość importu plików MIB o Przesyłanie alertów „as-is” do innych konsol firm trzecich o Możliwość definiowania ról administratorów o Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów o Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) o Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta o Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów o Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, 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. o Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. o Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile o Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. o Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. o Zdalne uruchamianie diagnostyki serwera. o Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. o Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. |  |
| **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.
* 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 Bronze według normy wprowadzonej w 2019 roku - **Złożę dokument potwierdzający spełnianie wymogu przed podpisaniem umowy.**

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 lub równoważne |  |
| **Dokumentacja użytkownika*** Zamawiający wymaga dokumentacji w języku polskim lub angielskim.

Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |  |
| **Warunki gwarancji**• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 5 lat. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 telefonicznie oraz przez Internet. • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. • Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon/portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • 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. • 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. |  |
| **Urządzenie typu 2 – macierz dyskowa – 1 sztuka** | **Typ obudowy** Macierz musi być przystosowana do montażu w szafie rack 19”, o wysokość maksymalnie 2U z możliwością instalacji min. 12 dysków 3.5 |  |
| **Przestrzeń dyskowa** Zainstalowane: * 4x dysk SSD SAS o pojemności min. 1,92TB, Hot-Plug

4x dysk HDD SAS o pojemności min. 8TB, Hot-Plug i prędkości obrotowej 7200 RPM |  |
| **Możliwość rozbudowy** Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 264 dysków twardych. |  |
| **Obsługa dysków** Macierz musi mieć możliwość obsługiwania dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5” jak również 3,5”.  |  |
| **Sposób zabezpieczenia danych** **•** Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping). • Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. • Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku). • Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków. |  |
| **Tryb pracy kontrolerów macierzowych** Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.  |  |
| **Pamięć cache** • Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. • Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. • Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat. |  |
| **Rozbudowa pamięci cache** • Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. • Jeśli do obsługi powyższych funkcjonalności dla całej pojemności urządzenia wymagane są licencje - muszą być one zawarte w ofercie. |  |
| **Interfejsy** Macierz musi posiadać, co najmniej 8 portów 25Gb SFP28 (4 porty na kontroler) |  |
| **Kable/wkładki** • 4x kabel 25Gb SFP28 typu DAC o długości 1m • 2x kabel 12Gb HD Mini-SAS/HD Mini-SAS min. 3m |  |
| **Zarządzanie** • Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego.• Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej. |  |
| **Zarządzanie grupami dyskowymi oraz dyskami logicznymi** • Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. • Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy. • Jeśli do obsługi powyższych funkcjonalności dla całej pojemności urządzenia wymagane są licencje - muszą być one zawarte w ofercie. |  |
| **Thin Provisioning** • Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. * Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP).

• Jeśli do obsługi powyższych funkcjonalności dla całej pojemności urządzenia wymagane są licencje - muszą być one zawarte w ofercie. |  |
| **Tiering** • Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS oraz między dyskami SAS i NL SAS. • Tiering musi obejmować wszystkie woluminy w danej puli dyskowej. • Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych. |  |
| **Wewnętrzne kopie migawkowe** • Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. • Macierz musi wspierać minimum 512 kopii migawkowych. Jeśli do obsługi powyższych funkcjonalności dla całej pojemności urządzenia wymagane są licencje - muszą być one zawarte w ofercie. |  |
| **Wewnętrzne kopie pełne** • Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Jeśli do obsługi powyższych funkcjonalności dla całej pojemności urządzenia wymagane są licencje - muszą być one zawarte w ofercie. |  |
| **Migracja danych w obrębie macierzy** Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeśli do obsługi powyższych funkcjonalności dla całej pojemności urządzenia wymagane są licencje - muszą być one zawarte w ofercie. |  |
| **Podłączanie zewnętrznych systemów operacyjnych**• Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). • Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix lub równoważne. • Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. • Jeśli do obsługi powyższych funkcjonalności dla całej pojemności urządzenia wymagane są licencje - muszą być one zawarte w ofercie. |  |
| **Redundancja**• Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. • Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. • Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy. • Zasilacze użyte w macierzy muszą spełniać wymagania dotyczące sprawności dla zasilacza minimum 80+ Gold.  |  |
| **Dodatkowe wymagania** • Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych. • Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie. |  |
| **Standardy bezpieczeństwa** Urządzenie musi spełniać następujące standardy bezpieczeństwa: EN 62368-1 (European Union), IEC 60950-1 (International) |  |
| **Inne** • Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego przed podpisaniem umowy, Wykonawca musi przedstawić oświadczenie producenta lub oficjalnego dystrybutora producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Dystrybutor taki musi posiadać aktualny certyfikat producenta stosownie do oferowanego sprzętu. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. • Deklaracja zgodności CE. |  |
| **Warunki gwarancji** • Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 5 lat. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 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. • 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. |  |
| **Urządzenie typu 3 – serwer – 2 sztuki** | **Obudowa** • Obudowa Rack o wysokości max 1U z możliwością instalacji do 8 dysków 2.5" Hot-Plug • Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. |  |
| **Płyta główna** • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Na płycie głównej musi znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci RAM o sumarycznej pojemności do 1TB |  |
| **Procesor** Zainstalowane dwa procesory 8-rdzeniowe, min. 3.2GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 135 w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org dla dwóch procesorów. |  |
| **RAM** 512 GB DDR4 RDIMM 3200MT/s lub lepsze |  |
| **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 |  |
| **Dyski twarde**Zainstalowane: 2x dysk SATA SSD o pojemności min. 480GB, Hot-Plug. |  |
| **Interfejsy sieciowe/ SAS** • Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet BaseT oraz 2 interfejsy sieciowe w standardzie SFP28 wspierające prędkości 10Gb oraz 25Gb (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) • Dwuportowa karta sieciowa z portami w standardzie SFP28 wspierające prędkości 10Gb oraz 25Gb |  |
| **Wbudowane porty** **•** Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej, • Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0 |  |
| **Wideo** Zintegrowana karta graficzna umożliwiająca wyświetlenie obrazu o rozdzielczości min. 1600x900 |  |
| **Wentylatory**Redundantne |  |
| **Zasilacze** Redundantne, Hot-Plug minimalnie 1100W klasy Titanium |  |
| **Elementy montażowe** Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych |  |
| **System operacyjny/dodatkowe oprogramowanie** Windows Server 2022 Datacenter licencje na 16 rdzeni, wersja polska i angielska lub równoważny |  |
| **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 wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem |  |
| **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 SSL • 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; • integracja z Active Directory; • 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 • możliwość obsługi przez sześciu użytkowników jednocześnie; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; •możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; 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 • ferowanego 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 • 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 • parciu 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. • 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 Bronze według normy wprowadzonej w 2019 roku - **Złożę dokument potwierdzający spełnianie wymogu przed podpisaniem umowy.**• 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 lub równoważne. |  |
| **Dokumentacja użytkownika** Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |  |
| **Warunki gwarancji** • Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 5 lat. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 telefonicznie oraz przez Internet. • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. • Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon/portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. • Zamawiający wymaga możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Zamawiający wymaga 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. |  |
| **Urządzenie typu 4 – macierz dyskowa – 1 sztuka** | **Typ obudowy** • Macierz musi być przystosowana do montażu w szafie rack 19”, o wysokość maksymalnie 2U z możliwością instalacji min. 12 dysków 3.5”  |  |
| **Przestrzeń dyskowa** Zainstalowane: • 6x dysk SSD SAS o pojemności min. 1,92TB, Hot-Plug • 6x dysk HDD SAS o pojemności min. 16TB, Hot-Plug i prędkości obrotowej 7200 RPM |  |
| **Możliwość rozbudowy** • Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 264 dysków twardych**.** |  |
| **Obsługa dysków** • Macierz musi mieć możliwość obsługiwania dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5” jak również 3,5”.  |  |
| **Sposób zabezpieczenia danych** • Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping). • Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. • Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku). • Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków. |  |
| **Tryb pracy kontrolerów macierzowych** • Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.  |  |
| **Pamięć cache** • Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. • Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi**.** • Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat. |  |
| **Rozbudowa pamięci cache** • Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. • Jeśli do obsługi powyższych funkcjonalności dla całej pojemności urządzenia wymagane są licencje - muszą być one zawarte w ofercie. |  |
| **Interfejsy** Macierz musi posiadać, co najmniej 8 portów 25Gb SFP28 (4 porty na kontroler) |  |
| **Kable/wkładki** • 4x kabel 25Gb SFP28 typu DAC o długości 1m • 2x kabel 12Gb HD Mini-SAS/HD Mini-SAS min. 3m |  |
| **Zarządzanie** Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej.  |  |
| **Zarządzanie grupami dyskowymi oraz dyskami logicznymi** • Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. • Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy. • Jeśli do obsługi powyższych funkcjonalności dla całej pojemności urządzenia wymagane są licencje - muszą być one zawarte w ofercie. |  |
| **Thin Provisioning** • Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. • Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP). • Jeśli do obsługi powyższych funkcjonalności dla całej pojemności urządzenia wymagane są licencje - muszą być one zawarte w ofercie |  |
| **Tiering** • Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS oraz między dyskami SAS i NL SAS. • Tiering musi obejmować wszystkie woluminy w danej puli dyskowej. • Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych. |  |
| **Wewnętrzne kopie migawkowe** • Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. • Macierz musi wspierać minimum 512 kopii migawkowych. Jeśli do obsługi powyższych funkcjonalności dla całej pojemności urządzenia wymagane są licencje - muszą być one zawarte w ofercie. |  |
| **Wewnętrzne kopie pełne** • Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. • Jeśli do obsługi powyższych funkcjonalności dla całej pojemności urządzenia wymagane są licencje - muszą być one zawarte w ofercie. |  |
| **Migracja danych w obrębie macierzy** • Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeśli do obsługi powyższych funkcjonalności dla całej pojemności urządzenia wymagane są licencje - muszą być one zawarte w ofercie |  |
| **Podłączanie zewnętrznych systemów operacyjnych** • Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). • Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix lub równoważne. • Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. • Jeśli do obsługi powyższych funkcjonalności dla całej pojemności urządzenia wymagane są licencje - muszą być one zawarte w ofercie |  |
| **Redundancja** • Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. • Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. • Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy. • Zasilacze użyte w macierzy muszą spełniać wymagania dotyczące sprawności dla zasilacza minimum 80+ Gold.  |  |
| **Dodatkowe wymagania** • Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych. • Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie. |  |
| **Standardy bezpieczeństwa** Urządzenie musi spełniać następujące standardy bezpieczeństwa: EN 62368-1 (European Union), IEC 60950-1 (International) |  |
| **Inne** Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego przed podpisaniem umowy, Wykonawca musi przedstawić oświadczenie producenta lub oficjalnego dystrybutora producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Dystrybutor taki musi posiadać aktualny certyfikat producenta stosownie do oferowanego sprzętu. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. • Deklaracja zgodności CE.  |  |
| **Warunki gwarancji** • Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 5 lat. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 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. • 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. |  |
| **Urządzenie typu 5 – Zestaw zasilania awaryjnego – 4 sztuki** | **Urządzenia** • Zestaw UPS typu Online podwójnej konwersji z akumulatorami litowo-jonowymi o żywotności co najmniej 5 lat • Czas podtrzymania przy 2kW obciążenia powinien być nie mniejszy niż 120 minut. • Każdy zestaw UPS wraz z ewentualnymi modułami EBM nie może zajmować więcej niż 6U miejsca w szafie Rack oraz ważyć nie więcej niż 75kg • Cały zestaw musi mieć możliwość montażu w szafie Rack oraz mieć możliwość konwersji do zestawu wolnostojącego |  |
| **Zasilanie** • Prąd wyjściowy musi być jednofazowy i mieć przebieg sinusoidalny o częstotliwości synchronizowanej z siecią elektryczną • Urządzenie musi obsługiwać na wejściu prąd jednofazowy, zgodny z polskimi normami • Zniekształcenia harmoniczne napięcia wyjściowego musi wynosić nie więcej niż 2% |  |
| **Inne** • Urządzenia muszą mieć możliwość bezpiecznego zamknięcia serwerów za pomocą dedykowanego oprogramowania • Dedykowane oprogramowanie ma wspierać system redundantnej pracy systemu UPS (klastra High-Availability urządzeń UPS) i bezpiecznego wyłączenia podłączonego klastra serwerów z systemem Windows Server 2022 lub równoważny• Urządzenia muszą mieć możliwość raportowania swojego stanu za pomocą SNMP przez sieć po złączu 1000BASE-T i wspierać uwierzytelnienie za pomocą LDAP oraz Radius |  |
| **Urządzenie typu 6 – serwer backupu – 2 sztuki** | **Zarządzanie i magazyny** 1. Sprzęt musi być fabrycznie nowy, rok produkcji nie starszy niż 2024 r.2. System powinien być dostarczony w ramach sprzętowego appliance z zainstalowanymi i skonfigurowanymi wszystkim usługami, niezbędnymi do pracy systemu.3. Rozwiązanie musi spełniać minimalne poniższe wymagania sprzętowe:a. Obudowa rack rozmiar: 2ub. Pamięć RAM: 32 GBc. Przestrzeń dostępna na przechowywanie danych (po odliczeniu straty pojemności wynikającej ze skonfigurowanej puli RAID oraz dysków systemowych): minimum 60TBd. Osobne dyski SSD M.2 nVME działające w RAID1 w celu instalacji warstwy oprogramowania i systemu operacyjnego,e. Redundantne zasilanie,Interfejsy sieciowe: 2szt 1 Gb oraz 2 szt. 25Gb.f. Gwarancja NBD on-premise o czasie trwania analogicznym do trwania wsparcia technicznego.4. Produkt dostępny w polskiej wersji językowej.5. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej6. System musi umożliwiać tworzenie kopii zapasowych na poziomie dysków7. System musi umożliwiać tworzenie kopii zapasowych na poziomie plików i folderów8. System musi umożliwiać replikację kopii zapasowych do wielu lokalizacji docelowych9. System musi umożliwiać tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT10. System musi umożliwiać współpracę z usługą kopiowania woluminów w tle (VSS) firmy Microsoft11. Możliwość zdefiniowania limitu przepustowości sieciowej z jakiej ma korzystać oprogramowanie backupowe12. System zarządzania nie może być oparty o relacyjne bazy danych.13. Rozwiązanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej).14. Rozwiązanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera (urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera (urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).15. Aplikacje klienckie powinny wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn – serwer backupu/usługa zarządzania, ani żaden inny element Systemu, nie powinien brać udziału w przesyłaniu danych.16. Rozwiązanie musi być systemem multi-storage-owym i umożliwia tworzenie wielu repozytoriów danych jednocześnie również na innych środowiskach jako przestrzeń do replikacji danych.17. System musi oferować mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.18. System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami.19. System musi umożliwiać wykonywanie kopii obrazu dysku, kopii plików i katalogów oraz kopii maszyn wirtualnych bez ich zatrzymywania z zachowaniem stuprocentowej integralności i spójności danych wewnątrz wykonanej kopii zapasowej.20. Rozwiązanie musi realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie.21. Rozwiązanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.22. System musi umożliwiać automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku wystąpienia błędu.23. Rozwiązanie powinno umożliwiać klonowanie planów kopii zapasowych, planów replikacji oraz planów testowego odtwarzania maszyn wirtualnych24. Rozwiązanie powinno umożliwiać uruchamianie przy zadaniach backupu dowolnych skryptów PRE/POST oraz po wykonaniu migawki VSS.25. System powinien umożliwiać definiowanie tzw. okna backupowego dla każdego z zadań w celu umożliwienia zarządzania obciążeniem sieci i uwzględnienia okien serwisowych występujących u Zamawiającego.26. System musi automatycznie dodawać do polityki i harmonogramu tworzenia backupów nowe źródła / maszyny wirtualnych, dodane do bieżącego środowiska (automatyzacja oparta na polityce tworzenia kopii).27. Rozwiązanie musi udostępniać możliwość podglądu postępu działania dowolnego zadania, w tym zadania wykonywania kopii zapasowych, odtwarzania danych, testowego odtwarzania danych, usuwania danych oraz zadania odświeżania zajętości magazynu na dane.28. Rozwiązanie musi posiadać system powiadamiania poprzez e-mail oraz Slack o zdarzeniach w następujących przypadkach: zadanie zostało zakończone pomyślnie, zadanie zostało zakończone z ostrzeżeniami, zadanie zostało zakończone z błędem, zadanie zostało anulowane, zadanie nie zostało uruchomione.29. System powinien umożliwiać wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika,30. Oferowane rozwiązanie musi być dobrane pod względem wydajności w oparciu o najlepsze praktyki producenta. 31. Rozwiązanie musi być wyskalowane, dobrane pod względem wymaganej funkcjonalności i wydajności stosownie do ilości zabezpieczanych danych i obiektów z uwzględnieniem przyrostu danych (serwery, maszyny wirtualne, bazy danych itp.) zgodnie z opisem w zapytaniu ofertowym. 32. Wydajność oferowanej konfiguracji musi być taka, aby wszystkie funkcje systemu były dostępne w chwili wdrożenia (np. deduplikacja, kompresja, instancja workerów i browserów, replikacja, testowe odtwarzanie maszyn wirtualnych).33. System pozwala na zmniejszenie rozmiaru przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych.34. Proces deduplikacji musi być możliwy dla każdego z typów obsługiwanych magazynów.35. Proces deduplikacji nie może wymagać instalacji żadnych dodatkowych komponentów, które będą pośredniczyły w zapisie danych z deduplikowanych 36. Proces deduplikacji nie może posiadać pojedynczego punktu awarii, tym samym musi być dostępny jednocześnie na każdym wspieranym magazynie na dane - również replikacyjnych. Awaria jednego z magazynów na dane nie może wpłynąć na integralność deduplikatów, jak i tablicy deduplikatów na innym magazynie.37. Proces deduplikacji realizowany jest blokiem o stałej wielkości, którego wielkość może zostać ustalona na etapie wdrożenia rozwiązania zgodnie z najlepszymi praktykami producenta.38. Proces szyfrowania kopii zapasowych nie może ograniczać procesu deduplikacji w ramach tego samego klucza szyfrującego.39. Kompresja kopii zapasowych musi obsługiwać jeden z wymienionych algorytmów: LZ4, ZStandard. Dodatkowo, musi umożliwiać określenie szczegółowego poziomu kompresji, w tym: niski, średni, wysoki.40. Instalacja, modyfikacja ustawień, polityki tworzenia kopii zapasowej systemu nie może wymagać przerwania pracy lub restartu systemu.41. System musi pozwalać na automatyczne aktualizacje oprogramowania.42. System musi być w stanie kompresować i szyfrować zabezpieczone dane w systemach NAS.43. System musi pozwalać na uruchomienie kontenerów Docker w dowolnych urządzeniach NAS i innych środowiskach w celu ich zabezpieczenia.44. System tworzenia kopii zapasowej musi przechowywać dane w sposób zapewniający ich niezmienność (tzw. "resilience"), dzięki czemu kopie zapasowe nie będą mogły zostać nadpisane lub zmodyfikowane przez cały okres ich przechowywania, retencji.45. System zarówno będzie przechowywać dane w kopii zapasowej w postaci zaszyfrowanej jak też ruch wewnątrz systemu również musi być szyfrowany.46. Archiwum długoterminowych kopii zapasowych musi być szyfrowane, a odzyskiwanie z archiwum obsługiwane z tego samego interfejsu użytkownika, co inne przywracanie dane.47. System musi mieć mechanizmy chroniące przejęcie konta administratora oraz umożliwiać definiowanie dodatkowych uprawnień dla każdej z predefiniowanych ról użytkowników.48. System musi pozwalać na gradację uprawnień administratorów - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: system operator, backup operator, restore operator, viewer. Dla każdej z tych ról system musi umożliwiać przypisywanie dodatkowych uprawnień, w tym możliwość zablokowania usuwania danych.49. Rozwiązanie musi posiadać możliwość nieodwracalnego usuwania danych z magazynu na dane w momencie spełnienia dodatkowych wymogów.50. W sytuacji, gdyby podstawowe urządzenie tworzenia kopii zapasowej było niedostępne, system musi posiadać możliwość przywrócenia z archiwum za pomocą innej instancji systemu dostarczonej przez tego samego producenta. tzn. archiwum musi zawierać wszystkie informacje konieczne do odzyskania.51. Rozwiązanie musi umożliwiać uruchomienie konsoli w chmurze producenta zlokalizowanej na terenie Polski, w celu umożliwienia dostępu do środowiska zarządzania kopiami zapasowymi w przypadku czasowej niedostępności środowiska lokalnego.52. System kopii zapasowej musi umożliwiać dostęp do konsoli administracyjnej z wielu stacji roboczych.53. System kopii zapasowej musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.54. System powinien posiadać predefiniowane schemat tworzenia kopii zapasowych, min. Custom, Basic, G-F-S, Forever incremental,55. Rozwiązanie musi obsługiwać kontrolę dostępu opartą na rolach (RBAC).56. Możliwość składowania utworzonych kopii zapasowych na magazynach chmurowych Amazon AWS, Azure, Wasabi, Google Cloud Storage, Backblaze B2, magazyny zgodne z S3 oraz dedykowana chmura producenta appliance’u57. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych po protokole smb,S3, nfs, iscsi, katalog lokalny58. Zarządzanie i odzyskiwanie danych z kopii musi odbywać się z tego samego interfejsu użytkownika (konsoli), niezależnie od tego, gdzie znajduje się kopia zapasowa (w chmurze AWS, Azure, GCP, w Data Center czy w usłudze typu SaaS).59. Czas przechowywania kopii zapasowej (retention time) systemu backupu nie może być zmieniony np. poprzez manipulowanie wskazaniami zegara serwera NTP w celu szybszego ich wyekspirowania - tzn. czasy przechowywania kopii zapasowych nie będą zależne od wskazań zegara czasu serwera NTP, ale będą wykorzystywać technologię, która mierzy upływ czasu.60. Możliwość generowania raportów dobowych w oparciu o harmonogram61. Produkt musi posiadać możliwość zapisu kopii zapasowych do magazynu chmurowego dostarczanego bezpośrednio przez producenta oprogramowania (datacenter powinno być zlokalizowane na terenie Polski) 62. Produkt musi posiadać możliwość zdefiniowania maksymalnej liczby równocześnie backupowanych urządzeń w ramach jednego planu backupowego, niezależnie od typu urządzenia (np. stacja robocza, serwer, maszyna wirtualna)63. Możliwość wyświetlenia szczegółowych informacji o chronionym urządzeniu takich jak: CPU, RAM, System operacyjny, Adres IP.64. Produkt musi posiadać możliwość zdefiniowania poziomu obciążenia magazynu, po osiągnięciu którego zostanie wysłane powiadomienia e-mail. (poziom definiowany indywidualnie dla każdego magazynu) |  |
| **Wspierane systemy**Możliwość instalacji oraz uruchomienia agenta backupowego na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy:Windows: 7, 8.1, 10(1607+), (lub równoważny)Windows Server: 2008 R2+, (lub równoważny)Środowisk wirtualnych:Hyper-V 2016+, (lub równoważny)VMware: 6.7+. (lub równoważny) |  |
| **Środowiska fizyczne i bazy danych**1. Rozwiązanie powinno umożliwiać tworzenie grup urządzeń w celu automatyzacji procesów podczas pracy z urządzeniami.2. Produkt musi posiadać możliwość tworzenia zadań dla grupy urządzeń oraz dla wybranych urządzeń. 3. Rozwiązanie musi pozwalać na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej.4. Rozwiązanie backupowe musi pozwalać na zabezpieczanie zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption.5. System jest niezależny od wersji Microsoft SQL i musi umożliwiać przywracanie danych SQL dla tej samej lub nowszej wersji.6. System musi obsługiwać również narzędzia RMAN firmy Oracle do tworzenia kopii zapasowych i odzyskiwania. Dodatkowo system musi obsługiwać funkcję przyrostowego scalania danych.7. System kopii zapasowej musi wspierać odtwarzanie pojedynczych plików z systemów Windows oraz Linux.8. W przypadku niedostępności źródła danych, system musi oczekiwać na powrót dostępności źródła danych przez określony przez administratora okres. W przypadku braku powrotu dostępności źródła, system musi podjąć ustaloną przez administratora liczbę prób kontynuacji kopii. W przypadku powrotu źródła danych system musi kontynuować zadanie backupu od momentu, w którym wystąpiła niedostępność źródła - system nie może rozpoczynać zadania od punktu początkowego i rozpoczynać przesyłania kopii od zera. W przypadku braku powrotu źródła danych system powinien zakończyć zadanie błędem.9. Odtwarzanie Bare Metal Restore w Systemie może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.10. Rozwiązanie powinno umożliwiać uruchamianie procesu Bare Metal Restore z dowolnego bootowalnego nośnika danych.11. Rozwiązanie powinno wspierać odtwarzanie danych w scenariuszach P2P, P2V, V2P, V2V.12. Rozwiązanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie (RAW, VHD, VHDX, VMDK).13. Rozwiązanie musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL) oraz z prawami dostępu. Funkcjonalność ta musi być możliwa do skonfigurowania przez administratora na etapie konfiguracji procesu przywracania danych.14. Rozwiązanie musi umożliwiać przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows). |  |
| **Środowiska wirtualne**1. System musi wspierać kopię w trybie application-aware dla wszystkich wspieranych wirtualizatorów.2. System musi umożliwiać wykonywanie kopii maszyn wirtualnych z zastosowanie zaawansowanych metod transportu (HotAdd, SAN, LAN), w tym metodami LAN-Free, tj. takimi, które podczas wykonywania backupu nie obciążają interfejsów sieciowych maszyn wirtualnych.3. System kopii zapasowej musi wykorzystywać mechanizmy Change Block Tracking oraz Replica Change Tracking dla wspieranych przez producenta platformach wirtualizacyjnych. 4. Rozwiązanie producenta musi być certyfikowane przez dostawcę platformy wirtualizacyjnej, tj. producent musi uczestniczyć w programie Technology Alliance Partner.5. System kopii zapasowej musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage-u użytego do przechowywania kopii zapasowych.6. Dla środowiska vSphere i Hyper-V rozwiązanie powinno umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).7. System kopii zapasowej musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere.8. System kopii zapasowej musi umożliwiać weryfikację odtwarzalności wirtualnych maszyn według własnego harmonogramu w dowolnym środowisku. |  |
| **Aplikacje SaaS**1. Ochrona z tej samej konsoli dla Microsoft 365 minimum na poziomie, skrzynek pocztowych, onedrive, kontaktów, kalendarza.2. Rozwiązanie musi umożliwiać przywracanie danych Microsoft 365: do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku .pst oraz do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji)3. System musi umożliwiać granularne odtwarzanie danych, tj. pojedynczych plików z kopii obrazu dysku oraz pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365.4. System musi umożliwiać zabezpieczanie środowisk Git, w tym GitHub, GitLab oraz Bitbucket wraz z metadanymi5. System musi umożliwiać odtworzenie dowolnego środowiska Git w dowolnym innym środowisku Git, tzw. odtwarzanie crossowe.6. System musi umożliwiać zabezpieczenie metadanych zebranych wokół repozytorium w ramach zabezpieczanego środowiska Git.7. System musi umożliwiać odtwarzanie metadanych repozytorium Git do dowolnego innego środowiska Git w przypadku chęci odtworzenia repozytorium.8. System musi umożliwiać zabezpieczenie środowisk Jira9. System musi umożliwiać odtworzenie środowiska Jira do chmury lub środowiska lokalnego. |  |
| **Licencjonowanie i wsparcie techniczne**1. Wszystkie linie supportu muszą być obsługiwane w języku polskim.2. Wsparcie techniczne musi być świadczone bezpośrednio przez główną siedzibę producenta minimum przez 60 miesięcy.3. Możliwość zgłaszania ticketów supportowych bezpośrednio z poziomu interfejsu zarządzania w formie czatu.4. Wsparcie techniczne musi być świadczone w modelu 24/7.5. Producent wraz z rozwiązaniem musi udostępnić materiały samopomocowe w j. polskim (minimum dostęp do bazy wiedzy, materiałów wideo oraz kart produktów)6. Wsparcie techniczne musi umożliwiać korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego.7. W ramach wsparcia technicznego Zamawiający musi mieć dostęp do tzw. Dedicated Customer Success Managera, tj. osoby po stronie Dostawcy dedykowanej do obsługi zgłoszeń technicznych, doraźnej pomocy i bieżącej pomocy w utrzymania infrastruktury Zamawiającego.8. W ramach dokumentacji posprzedażowej Dostawca musi dostarczyć bezpośredni numer telefonu oraz adres e-mail do Dedicated Customer Success Managera.9. Licencje w ramach rozwiązania powinny pozwalać na zabezpieczenie: nielimitowanej ilości maszyn wirtualnych, nielimitowanej ilości serwerów fizycznych, nielimitowanej ilości stacji roboczych.10. Licencje powinny być dostępne w opcji wieczystej. Wsparcie techniczne nie powinno być wymagane dla poprawnego działania systemu. |  |
| **Anty-ransomware i bezpieczeństwo**1. System plików rozwiązania musi być odporny na ataki Ransomware (zapewnić ochronę przed szyfrowaniem end-to-end, kopie zapasowe nie mogą być nadpisywane - "niezmienny system plików").2. System powinien umożliwiać wykorzystanie wbudowanego menedżera haseł do przechowywania wszelkich sekretów (haseł, danych dostępowych, kluczy szyfrujących) wykorzystywanych przez System3. System powinien umożliwiać przywrócenie hasła głównego administratora w przypadku jego utraty.4. W ramach systemu, komunikacja pomiędzy hostem źródłowym, a magazynem powinna odbywać się tylko i wyłącznie bezpośrednio pomiędzy agentem backupu, a magazynem. Komunikacja nie może przechodzić przez serwer backupu, ani żaden inny komponent, którego awaria sparaliżowałaby działanie Systemu. System nie może posiadać pojedynczego punktu awarii.5. System musi działać w zgodzie z regułą Zero-knowledge Encryption. Oznacza to, że wszelkie sekrety muszą być przechowywane w centralnym Managerze Haseł w postaci zaszyfrowanej algorytmem AES i być udostępniane agentowi dopiero w momencie rozpoczęcia wykonywania kopii zapasowej. Sekrety nie mogą być przechowywane w konfiguracji agenta na zabezpieczanym urządzeniu |  |
| **Microsoft Windows Server 2022 USER CAL lub równoważny** | 150 szt. |  |
| **Microsoft SQL Server 2022 Standard Edition (zawiera 5 USER CAL) wersja polska lub angielska lub równoważny** | 2 szt. |  |
| **Microsoft SQL Server 2022 USER CAL lub równoważny** | 70 szt. |  |
| **Microsoft Windows Server 2022 RDS USER CAL lub równoważny** | 10 szt. |  |
| Macierz, serwery oraz rozwiązanie backupu (urządzenia typu 1-4 oraz 6) muszą mieć możliwość zarządzania i monitoringu oraz aktualizacji oprogramowania firmware z poziomu jednego środowiska zarządczego producenta sprzętu. Oprogramowanie to musi posiadać przynajmniej funkcjonalności takie jak:• Wykrywanie innych urządzeń w środowisku datacenter• Widok zasobów sprzętowych oraz kondycji innych urządzeń• Podgląd i zarządzanie powiadomieniami oraz regułami ich otrzymywania• Podgląd wersji sterowników systemu oraz podzespołów wraz z możliwością ich aktualizacji• Wymuszanie zdalnych zadań: restart, uruchomienie oraz zamknięcie systemu• Możliwość przenoszenia ustawień pomiędzy urządzeniami za pomocą szablonów • Wykrywanie różnic w ustawieniach pomiędzy urządzeniami za pomocą puli identyfikacji• Monitorowanie ważności gwarancji wszystkich urządzeń• System zarządzania musi obsługiwać dostęp przez wielu użytkowników oraz mieć możliwość:o Autentykacji za pomocą LDAP, OIDCo Limitowania dostępu do konsoli oraz akcji opartych na rolacho Limitowania dostępu do urządzeń w zależności od grup, do których one należą• Wszystkie dane wrażliwe przetwarzane przez system zarządzający muszą być przechowywane w formie zaszyfrowanej• Zewnętrzny ruch sieciowy musi być szyfrowany za pomocą HTTPS• Wsparcie dla systemów oraz wykrywanie urządzeń z tymi systemami operacyjnymi:o Microsoft Windows Systems Center 2025 lub równoważnyo Microsoft Windows 2025 lub równoważnyo SUSE 15 SP6o Ubuntu 24.04.4o RHEL 9.4 |  |

1. Oświadczam, że zapoznałem się z treścią zapytania ofertowego oraz że nie wnoszę zastrzeżeń do jego treści i zdobyłem wszelkie informacje niezbędne do sporządzenia oferty i wykonania zamówienia. Złożona oferta spełnia wszelkie parametry i warunki zapytania ofertowego.
2. Oświadczam, że akceptuję termin związania ofertą wynoszący 30 dni od dnia upływu terminu składania ofert, przy czym pierwszym dniem terminu związania ofertą jest dzień, w którym upływa termin składania ofert.
3. Zobowiązuje się wykonać zamówienie w terminach wskazanych w Zapytaniu ofertowym,
4. W przypadku wyboru mojej oferty zobowiązuję się do zawarcia umowy na wykonanie przedmiotu zamówienia w miejscu i terminie wskazanym przez Zamawiającego.
5. Umowa będzie opiewać na kwotę brutto.
6. Znajduję się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia.
7. Posiadam wiedzę i doświadczenie niezbędne do realizacji przedmiotu zamówienia.
8. Wyrażam zgodę na przetwarzanie przez Zamawiającego danych osobowych na potrzeby realizacji niniejszego postępowania zgodnie z art. 23 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 ze zm.) do celów związanych z przeprowadzeniem niniejszego postępowania. Moja zgoda obejmuje również przetwarzanie danych w przyszłości pod warunkiem, że nie zostanie zmieniony cel przetwarzania.
9. Jestem świadomy/-a odpowiedzialności karnej za fałszywe zeznania wynikające z art. 233 (podanie nieprawdy lub zatajenie nieprawdy) ustawy z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 1997 r., Nr 88, poz. 553 ze zm.), a zawarte w ofercie informacje są zgodne z prawdą oraz stanem faktycznym.

………….……………………………

Czytelny podpis osoby uprawnionej do reprezentowania podmiotu

Załączniki:

1. Załącznik nr 2 – oświadczenie Wykonawcy – warunki udziału w postępowaniu
2. Załącznik nr 3 – wykaz dostaw
1. Zakres danych i informacji musi także potwierdzać **równoważność** oferowanych urządzeń, w stosunku do wymagań wskazanych przez Zamawiającego [↑](#footnote-ref-2)