

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Na potrzeby niniejszego OPZ wraz z załącznikami dotyczącej opisanego zamówienia, wymienionym w niniejszym paragrafie pojęciom nadają znaczenie określone poniżej, oraz że użyte w tekście poniżej wymienione pojęcia, rozumiane będą w sposób poniżej zdefiniowany. Dla podkreślenia, że pojęcia te rozumiane są w sposób zdefiniowany, ich pierwsze litery będą pisane w tekście wielką literą.

Strony ustalają następujące definicje:

1. **Zamawiający** – Szpital Specjalistyczny im. Świętej Rodziny SPZOZ w Warszawie. 02-544 Warszawa, ul. Madalińskiego 25, zwany dalej Szpital.
2. **Wykonawca** - podmiot, który ubiega się o udzielenie zamówienia, złożył ofertę albo zawarł umowę w postępowaniu o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego na podstawie art. 132 Ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (tj. Dz.U. z 2022 r. poz. 1710 z późn. zm.).
3. **Strony** - podmioty bezpośrednio uczestniczące w umowie zawiązanej na podstawie rozstrzygnięcia postępowania przetargowego.
4. **System informatyczny** - zbiór powiązanych ze sobą elementów, którego funkcją jest przetwarzanie danych przy użyciu techniki komputerowej. W skład systemu wchodzi najczęściej elementy: sprzęt komputerowy, oprogramowanie narzędziowe, oprogramowanie dziedzinowe.
5. **Infrastruktura sprzętowa** - znajdująca się w dyspozycji Zamawiającego, w tym stanowiąca jego własność oraz dostarczana w ramach realizacji przedmiotu zamówienia infrastruktura przetwarzania danych wszystkie połączenia, urządzenia fizyczne i oprogramowania aplikacyjne, które łącznie współpracując umożliwiają gromadzenie, przechowywanie, wytwarzanie danych i usług oraz udostępnianie danych i usług elektronicznych.
6. **Umowa** – umowa zawarta w wyniku rozstrzygnięcia postępowania o udzielenie zamówienia publicznego.
7. **SWZ** – Specyfikacja Warunków Zamówienia
8. **Gwarancja i Serwis Oprogramowania** – Oznacza całokształt świadczonych przez Wykonawcę usług (gwarancyjno-serwisowych) związanych z zapewnieniem poprawnej pracy składników będących przedmiotem zamówienia, szczegółowo określone w niniejszym dokumencie w oraz w projekcie umowy.
9. **Gwarancja i Serwis Infrastruktury Sprzętowej** – Oznacza całokształt świadczonych przez Wykonawcę usług (gwarancyjno-serwisowych) związanych z zapewnieniem poprawnej pracy składników będących przedmiotem zamówienia, szczegółowo określone w niniejszym dokumencie oraz w projekcie umowy.
10. **System Komunikacyjny** – infrastruktura telekomunikacyjna, sieciowa, systemy separacji, systemy bezpieczeństwa oraz certyfikaty serwerów WWW, obejmujące elementy lokalnej sieci komputerowej, łącza i urządzenia rozległej sieci transmisji danych oraz urządzenia komutacji pakietów wraz z ich oprogramowaniem.
11. **Oprogramowanie Narzędziowe** – elementy oprogramowania zainstalowane na sprzęcie komputerowym, obejmujące w szczególności:
 - systemy operacyjne (np. Windows, LINUX, UNIX),
 - system zarządzania bazą danych (SZBD), zwane też oprogramowaniem bazodanowym (np. MSSQL, Oracle),
 - oprogramowanie służące do administracji i zarządzania sprzętem komputerowym, systemem operacyjnym i systemem zarządzania bazą danych,

– oprogramowanie komunikacyjne umożliwiające podłączenie stacji dostępowych do serwera bazy;

12. **Systemy Zewnętrzne** – systemy z którymi docelowo współpracować będzie wdrażany system.

13. **Wdrożenie** – etap cyklu życia systemu informatycznego, polegający na instalacji i dostosowaniu oprogramowania do wymagań Zamawiającego.

- Podstawowe etapy procesu wdrożenia:
- Przygotowanie i skonfigurowanie infrastruktury technicznej,
- Wirtualizacja,
- Migracja,
- Backup.

14. **Zakończenie wdrożenia** – moment podpisania przez Zamawiającego Protokołu odbioru potwierdzającego wykonanie przez Wykonawcę wszystkich prac opisanych w OPZ bez jakichkolwiek uwag ze strony Zamawiającego.

15. **Zdalny Dostęp** – analogowe lub cyfrowe łącze wydajnej transmisji danych pomiędzy węzłem infrastruktury siedziby Wykonawcy, a węzłem infrastruktury zapewnianym przez Zamawiającego, umożliwiające realizować usługi serwisowe lub konfiguracyjne.

16. **Zadanie** – przedmiot zamówienia (przedmiot Umowy) wynikający łącznie z SWZ, Oferty Wykonawcy, Umowy.

17. **Protokół Dostawy** - protokół przygotowany przez Wykonawcę, będący potwierdzeniem przyjęcia przez Zamawiającego określonego sprzętu lub oprogramowania wymaganego w OPZ. Protokół musi zawierać dokładny opis dostarczonego sprzętu, symbol producenta, ilość sztuk oraz numery seryjne.

18. **Protokół odbioru końcowego**, zwany dalej: Protokołem dostawy, montażu i odbioru końcowego – protokół, będący potwierdzeniem przyjęcia przez Zamawiającego sprzętu, oprogramowania oraz wykonanych przez Wykonawcę prac będących przedmiotem umowy - sporządzony wg wzoru stanowiącego Załącznik nr 4 do umowy.

19. **Dzień Roboczy** – każdy dzień od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy.

20. **Godziny Robocze** – godziny od 7:00 do 15:00 w każdym Dniu Roboczym.

21. **Kierownik Zamawiającego** – osoba wyznaczona przez Zamawiającego, koordynująca realizację przedmiotu umowy, odpowiednio umocowana, w szczególności odpowiedzialna ze strony Zamawiającego za realizację przedmiotu zamówienia.

22. **Kierownik Wykonawcy** - osoba wyznaczona przez Wykonawcę do koordynacji realizacji prac danego zadania oraz upoważniona do podpisywania Dokumentacji Projektu z ramienia Wykonawcy.

DOSTAWA INFRASTRUKTURY SPRZĘTOWEJ ORAZ OPROGRAMOWANIA

Zakres rzeczowy zadania obejmuje modernizację infrastruktury serwerowni w Budynku Głównym Szpitala Specjalistycznego im. Świętej Rodziny SPZOZ w Warszawie przy ul. Madalińskiego 25; tj. zakup sprzętu i oprogramowania wraz z konfiguracją niezbędnych aplikacji, usługę wirtualizacji, migracji oraz backupu.

Ponadto w ramach dostaw zakres rzeczowy zadania zawiera:

- 1) Zakup serwerów bazodanowych – 2 szt.;
- 2) Zakup serwerów aplikacji – 4 szt.;
- 3) Zakup macierzy wydajnościowych – 2 szt.;
- 4) Zakup przełączników SAN z niezbędnym okablowaniem i wkładkami FC – 2 szt.;
- 5) Zakup oprogramowania serwerowego – 8 szt.;
- 6) Zakup oprogramowania bazodanowego – 2 szt.;

Poniżej wyspecyfikowano minimalne parametry sprzętu oraz oprogramowania, które należy dostarczyć w ramach realizacji przedmiotu zamówienia. W przypadku, gdy nie określono, że parametr określa maksymalną wartość jest to jego wartość minimalna.

Wymagania ogólne:

- 1) Całość dostarczanego sprzętu i oprogramowania standardowego musi pochodzić z autoryzowanego kanału sprzedaży producenta.
- 2) Całość dostarczanego rozwiązania, tzn. każde z dostarczonych urządzeń, musi być nowe, wcześniej nieużywane, rok produkcji nie starszy niż 2022.
- 3) Całość przedmiotu zamówienia, musi być objęte minimum 60-miesięczną gwarancją.
- 4) Urządzenia i ich komponenty muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu, producenta, jak i daty produkcji danego elementu.
- 5) Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej w języku polskim lub angielskim.
- 6) Do każdego urządzenia musi być dostarczony niezbędny sprzęt eksploatacyjny (przewody zasilające, przewody sygnałowe itp.) niezbędny do uruchomienia danego urządzenia w budowanym rozwiązaniu w miejscu dostawy wskazanym przez Zamawiającego. Sprzęt, o którym mowa powyżej jest integralną częścią oferty i przechodzi na własność Zamawiającego.
- 7) Wszystkie urządzenia muszą posiadać oznakowanie CE.
- 8) Wszystkie dostarczane urządzenia na dzień złożenia oferty nie mogą być w fazie end-of-life (EOL)
- 9) Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V \pm 10%, 50 Hz.
- 10) Wymagane jest, aby infrastruktura sprzętowa była gotowym produktem posiadającym nazwę handlową i złożonym z zamkniętej, ściśle zdefiniowanej listy komponentów posiadających odpowiednie numery katalogowe.
- 11) Dostarczane oprogramowanie musi zostać dostarczone w najnowszej stabilnej wersji, która uzyskała certyfikację producenta dostarczanego sprzętu (jeśli podlega certyfikacji).
- 12) Wykonawca, w celu zabezpieczenia danych krytycznych przetwarzanych w systemach medycznych Zamawiającego w czasie wdrożenia oraz migracji systemów na nowy sprzęt, zobowiązany jest na wezwanie Zamawiającego przedstawić dokumenty potwierdzające partnerstwo z firmą Asseco Poland producenta systemu medycznego, z którego obecnie korzysta Zamawiający.

Zamawiający wymaga, aby Wykonawca realizując opisane w przedmiocie zamówienia dostawy i usługi uwzględnił uwarunkowania środowiska aktualnie pracującego u Zamawiającego.

Wykonawca w ramach postępowania zobowiązany jest do wykonania następujących usług związanych z montażem i konfiguracją dostarczanej infrastruktury sprzętowej:

- 1) Konfiguracja serwerów, macierzy dyskowych oraz przełączników.
- 2) Instalacja oraz konfiguracji oprogramowania.
- 3) Dostarczenie dokumentacji powykonawczej infrastruktury sprzętowej i oprogramowania standardowego, która będzie składała się co najmniej z następujących elementów:

- Specyfikacja techniczna wraz z numerami katalogowymi poszczególnych elementów oraz numerami seryjnymi poszczególnych elementów,
- Końcowe nazwy oraz szczegółowa adresacja poszczególnych elementów,
- Konfiguracja środowiska wraz z połączeniami, konfiguracją poszczególnych elementów w tym logiczną konfiguracją miejsc
- Szczegóły dotyczące instalacji i uruchomienia infrastruktury sprzętowej, w zakresie modernizacji infrastruktury Zamawiającego, zostaną ustalone pomiędzy Stronami w trakcie Analizy Przedwdrożeniowej.
- Po zakończonym montażu Wykonawca prześle Zamawiającemu wszystkie hasła dostępowe do kont „super użytkowników” (kont administracyjnych).

Przedmiot dostawy :

- 1) Zakup serwerów bazodanowych – 2 szt.;
- 2) Zakup serwerów aplikacji – 4 szt.;
- 3) Zakup macierzy wydajnościowych – 2 szt.;
- 4) Zakup przełączników SAN z niezbędnym okablowaniem i wkładkami FC – 2 szt.;
- 5) Zakup oprogramowania serwerowego – 8 szt.;
- 6) Zakup oprogramowania bazodanowego – 2 szt.;

Asortyment	Minimalne parametry wymagane
Serwer bazodanowy – 2 sztuki	
Obudowa	Do instalacji w szafie Rack 19", wysokość nie więcej niż 1U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. Możliwość instalacji ramienia do zarządzania kablami.
Procesor	Architektura x86, maksymalny TDP dla procesora – maksymalnie 150W. Wymagana ilość rdzeni dla procesora – 16 z możliwością zmniejszenia ilości rdzeni w UEFI. Minimalna częstotliwość pracy procesora 2.0GHz. Minimalna częstotliwość w trybie Turbo / Boost – 4.0GHz. Minimalna ilość kanałów procesora – 8. Ilość kości pamięci na kanał – 2. Wynik wydajności procesora zainstalowanego w oferowanym serwerze nie powinien być niższy niż 276 punkty base w teście SPECrate 2017 Integer, opublikowanym przez SPEC.org (www.spec.org). Test przeprowadzony przez producenta serwera musi być zamieszczony na stronie spec.org. (do oferty należy załączyć wydruk ze strony z wynikiem testu).
Liczba procesorów	1
Płyta główna	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania minimum dwóch procesorów wykonujących 64-bitowe instrukcje. Możliwość instalacji 2 procesorów, po 60 rdzeni każdy.
Pamięć operacyjna	Zainstalowane minimum 256GB pamięci RAM o częstotliwości 4800MHz. Obsadzenie kości musi zagwarantować tzw. zbalansowane obsadzenie kości. Minimum 32 sloty na pamięć. Możliwość rozbudowy do 8TB RAM.
Zabezpieczenie pamięci	ECC, SDDC, ADDDC, Memory Mirroring

Procesor Graficzny	Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz. 1 port VGA na tylnym panelu. Możliwość zainstalowania drugiego portu VGA na przednim panelu serwera.
Rozbudowa dysków	W chwili dostawy serwer musi posiadać zainstalowane minimum <ul style="list-style-type: none"> • 4 sztuki dysku SSD o pojemności minimum 960GB każdy. Dyski z parametrem DWPD minimum 1,5. Serwer w chwili dostawy musi posiadać backplane obsługujący do 8 dysków 2,5" SAS/SATA. Wymagana możliwość instalacji minimum dysków M.2 zabezpieczonych sprzętowym RAID. Wymagany jest wewnętrzny slot na kartę Micro SD.
Kontroler dyskowy	W momencie dostawy serwer musi posiadać sprzętowy kontroler dyskowy obsługujący minimum RAID - 0/1/10/5. Kontroler nie może zajmować żadnego ze slotów I/O wyszczególnionych w sekcji „Dodatkowe sloty I/O”
Zasilacz	Minimum dwa redundantne zasilacze o mocy minimum 1100W z certyfikatem minimum Platinum.
Interfejsy sieciowe	Zainstalowana dwuportowa karta 10/25Gb, wyposażona we wkładki 10Gb. Karta nie może zajmować żadnego ze slotów PCIe. Zainstalowana dwuportowa karta FC 16Gb.
Dodatkowe sloty I/O	Serwer w chwili dostawy musi posiadać minimum 2 sloty PCIe Gen4 x16
Dodatkowe porty	<ul style="list-style-type: none"> • z przodu obudowy: 1x USB 3.2, 1x USB 2.0 (z możliwością zarządzania serwerem), zewnętrzny dedykowany port diagnostyczny, możliwość instalacji portu VGA. • z tyłu obudowy: 2x USB 3.2, 1x USB 2.0 1x VGA, 1x RJ-45 do zarządzania serwerem. Możliwość instalacji portu DB9. • wewnątrz obudowy: 1x USB 3.2. Wszystkie tylne porty USB, port RJ-45 służący do zarządzania, tylny port VGA, wewnętrzny port USB, wewnętrzny port na kartę Micro SD powinny być umieszczone na osobnej dedykowanej płycie I/O, którą łączy się bezpośrednio z płytą główną serwera.
Chłodzenie	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1
Zarządzanie	Możliwość instalacji zintegrowanego panelu LCD umożliwiającego wyświetlenie poniższych informacji: <ul style="list-style-type: none"> • aktywne ostrzeżenia; • Status serwera; • Typ oraz model serwera, numer seryjny; • Wersje oprogramowania UEFI oraz modułu zarządzania; • Informacje nt. modułu zarządzania: nazwa hosta, adres MAC, adres IP, adres DNS; • Dane środowiskowe: temperaturę procesora, poziom napięcia wejściowego, poziom zużycia energii; • Aktywne sesje połączeniowe do interfejsu zarządzania.

	<p>Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania, który musi być umieszczony na osobnej dedykowanej płycie I/O (wspomnianej w sekcji Dodatkowe Porty). Płyta I/O musi posiadać swój własny min. 2 rdzeniowy procesor o taktowaniu min. 1.2GHz.</p> <ul style="list-style-type: none"> • Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna). • Pozyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres IP karty zarządzającej, użycie CPU, użycie pamięci oraz komponentów I/O, lokalizacja. • Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów. • Logowanie zdarzeń związanych z utrzymaniem systemu jak upgradefirmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń. • Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3. • Update systemowego firmware. • Monitoring i możliwość ograniczenia poboru prądu. • Zdalne włączanie/wyłączanie/restart. • Zapis video zdalnych sesji. • Podmontowanie lokalnych mediów z wykorzystaniem Java Client. • Przekierowanie konsoli szeregowej przez IPMI. • Zrzut ekranu w momencie zawieszenia systemu. • Możliwość przejęcia zdalnego ekranu. • Możliwość zdalnej instalacji systemu operacyjnego. • Alerty Syslog. • Przekierowanie konsoli szeregowej przez SSH. • Wyświetlanie danych aktualnych i historycznych dla użycia energii oraz temperatury serwera. • Możliwość mapowania obrazów ISO z lokalnego dysku operatora. • Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS. • Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę. • Wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API. • Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzająca) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego. • Kontroler zarządzania musi posiadać 4Gb wewnętrznej
--	--

	<p>pamięci (dopuszcza się zastosowanie karty Micro SD w celu uzyskania tej pojemności). Pamięć kontrolera zarządzania musi pełnić funkcję RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware.</p> <ul style="list-style-type: none"> • Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot'u. • Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami. • Możliwość monitorowania i zarządzania grupą serwerów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200. <p>Wraz z serwerem powinno zostać dostarczone dodatkowe oprogramowanie zarządzające umożliwiające:</p> <ul style="list-style-type: none"> - zarządzanie infrastrukturą serwerów i storage bez udziału dedykowanego agenta; - przedstawianie graficznej reprezentacji zarządzanych urządzeń; - możliwość skalowania do minimum 1000 urządzeń; - obsługę szyfrowanej komunikacji z zarządzanymi urządzeniami, wsparcie dla NIST 800-131A oraz FIPS 140-2; - wsparcie dla certyfikatów SSL tzw. self-signed oraz zewnętrznych; - udostępnianie szybkiego podgląd stanu środowiska; - udostępnianie podsumowania stanu dla każdego urządzenia; - tworzenie alertów przy zmianie stanu urządzenia; - monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii; - konsola zarządzania oparta o HTML 5; - dostępność konsoli monitorującej na urządzeniach przenośnych ze wsparciem dla systemu Android oraz iOS, aplikacja musi umożliwiać włączenie wyłączenie oraz restart urządzenia, musi również mieć możliwość aktywowania diody lokacyjnej na urządzeniu; - automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja; - możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne dostępne na stronie producenta oferowanego rozwiązania; - definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzeń; - definiowanie roli użytkowników oprogramowania; - obsługa REST API oraz Windows PowerShell; - obsługa SNMP, SYSLOG, Email Forwarding; - autentykacja użytkowników: centralna (możliwość definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z MS AD oraz obsługa single
--	---

	<p>sign on oraz SAML;</p> <ul style="list-style-type: none"> - obsługa tzw. ForwardSecrecy w komunikacji z zarządzanymi urządzeniami; - przedstawianie historycznych aktywności użytkowników; - blokowanie możliwości podłączenia innego systemu zarządzania do urządzeń zarządzanych; - tworzenie dziennika zdarzeń ukończonych sukcesem lub błędem, oraz zdarzeń będących w trakcie. Możliwość definiowania filtrów wyświetlanych zdarzeń z dziennika. Możliwość eksportu dziennika zdarzeń do pliku csv; - Obsługa NTP; - przesyłanie alertów do konsoli firm trzecich; - tworzenie wzorców konfiguracji zarządzanych urządzeń (definiowanie przez konsole albo kopiowanie konfiguracji z już zaimplementowanych urządzeń); - instalowanie systemów operacyjnych oraz wirtualizatorów Vmware i Hyper-V. Wymagana jest integracja konsoli zarządzania z konsolą wirtualizatora tak, aby zarządzanie środowiskiem sprzętowym mogło odbywać się z konsoli wirtualizatora. Wymaga się możliwości instalacji systemu na przynajmniej 20 nodach jednocześnie. - możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta dla określonych zdarzeń wraz z przesyłem plików diagnostycznych. <p>Producent serwera ponadto powinien mieć w swojej ofercie narzędzia integrujące zarządzanie infrastrukturą z następującymi produktami: VMware, vCenter, Microsoft AdminCenter, Microsoft SystemCenter, RedHat CloudForms, Splunk.</p>
Funkcje zabezpieczeń	<p>Możliwość instalacji czujnika otwarcia obudowy zintegrowanego z modułem zarządzania serwerem, hasło włączania, hasło administratora, moduł RoT (umieszczony na dedykowanej płycie I/O wspomnianej w sekcji Dodatkowe porty) wspierający TPM2.0 oraz Platform FirmwareResiliency (PFR). Wymagana możliwość zainstalowania przedniego panelu zabezpieczającego zamykanego na klucz.</p>
Urządzenia hot swap	<p>Dyski twarde, zasilacze, wentylatory.</p>
Diagnostyka	<p>Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID.</p> <p>Możliwość użycia aplikacji mobilnej na telefonie, do przeglądania awarii, konfiguracji i włączenia/wyłączenia serwera.</p>
Systemy operacyjne	<p>Microsoft Windows Server 2019, 2022; Red Hat Enterprise Linux 8.6, 8.7, 9.0, 9.1, SUSE Linux Enterprise Server 15 SP4 oraz 15 Xen SP4; VMware vSphere (ESXi) 7.0 U3, ESXi 8.0; Ubuntu 22.04 LTS</p>
Waga	<p>maximum: 38.8kg</p>
Gwarancja	<p>60 miesięcy gwarancji producenta z oknem serwisowym 24x7. Czas</p>

	<p>reakcji serwisu – 4 godziny. Uszkodzone nośniki danych pozostają własnością zamawiającego. Możliwość wykupienia dodatkowego wsparcia, świadczonego przez producenta, z gwarantowanym czasem naprawy w ciągu 6 godzin. W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie Diagnostyka wymagane jest dostarczenie serwera nadmiarowego, mogącego zastąpić funkcjonalnie jak i wydajnościowo wymagane powyżej maszyny. Wszystkie komponenty serwera powinny być sygnowane i zoptymalizowane do użycia przez producenta serwera.</p> <p>Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu złożenia na wezwanie Zamawiającego oświadczenia, że w przypadku wystąpienia awarii nośnika danych w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony nośnik danych pozostaje u Zamawiającego. Dokument musi być oznaczony nazwą i numerem postępowania.</p> <p>Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych lub posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy złożyć na wezwanie Zamawiającego przed przystąpieniem do wykonywania Usług serwisowych. Dokument musi być oznaczony nazwą i numerem postępowania</p> <p>Potwierdzić, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta- Serwer musi być wyprodukowany zgodnie z normą ISO-9001 dokumenty należy dołączyć do oferty.</p> <p>Serwer musi posiadać deklaracja CE - dokument należy dołączyć do oferty.</p>
Serwer aplikacji – 4 sztuki	
Obudowa	Do instalacji w szafie Rack 19", wysokość nie więcej niż 1U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. Możliwość instalacji ramienia do zarządzania kablami.
Procesor	Architektura x86, maksymalny TDP dla procesora – maksymalnie 165W. Wymagana ilość rdzeni dla procesora – 20. Minimalna częstotliwość pracy procesora 2.0GHz. Minimalna częstotliwość w trybie Turbo / Boost – 3.9GHz. Minimalna ilość kanałów procesora – 8. Ilość kości pamięci na kanał – 2. Wynik wydajności procesora zainstalowanego w oferowanym serwerze nie powinien być niższy niż 349 punkty base w teście SPECrate 2017 Integer, opublikowanym przez SPEC.org (www.spec.org). Test przeprowadzony przez producenta serwera musi być zamieszczony na stronie spec.org. (do oferty należy załączyć wydruk ze strony z wynikiem testu).
Liczba procesorów	2
Płyta główna	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością

	zainstalowania minimum dwóch procesorów wykonujących 64-bitowe instrukcje. Możliwość instalacji 2 procesorów, po 60 rdzeni każdy.
Pamięć operacyjna	Zainstalowane minimum 256GB pamięci RAM o częstotliwości 4800MHz. Obsadzenie kości musi zagwarantować tzw. zbalansowane obsadzenie kości. Minimum 32 sloty na pamięć. Możliwość rozbudowy do 8TB RAM.
Zabezpieczenie pamięci	ECC, SDDC, ADDDC, Memory Mirroring
Procesor Graficzny	Zintegrowana karta graficzna z minimum 16MB pamięci osiągnięta rozdzielczość 1920x1200 przy 60 Hz. 1 port VGA na tylnym panelu. Możliwość zainstalowania drugiego portu VGA na przednim panelu serwera.
Rozbudowa dysków	W chwili dostawy serwer musi posiadać zainstalowane minimum <ul style="list-style-type: none"> • 4 sztuki dysku SSD o pojemności minimum 960GB każdy. Dyski z parametrem DWPD minimum 1,5. Serwer w chwili dostawy musi posiadać backplane obsługujący do 8 dysków 2,5" SAS/SATA. Wymagana możliwość instalacji minimum dysków M.2 zabezpieczonych sprzętowym RAID. Wymagany jest wewnętrzny slot na kartę Micro SD.
Kontroler dyskowy	W momencie dostawy serwer musi posiadać sprzętowy kontroler dyskowy obsługujący minimum RAID - 0/1/10/5. Kontroler nie może zajmować żadnego ze slotów I/O wyszczególnionych w sekcji „Dodatkowe sloty I/O”.
Zasilacz	Minimum dwa redundantne zasilacze o mocy minimum 1100W z certyfikatem minimum Platinum.
Interfejsy sieciowe	Zainstalowane dwuportowa karta 10/25Gb, wyposażone we wkładki 10Gb. Karta nie może zajmować żadnego ze slotów PCIe. Zainstalowana dwuportowa karta FC 16Gb.
Dodatkowe sloty I/O	Serwer w chwili dostawy musi posiadać minimum 3 slotyPCIe Gen4 x16.
Dodatkowe porty	<ul style="list-style-type: none"> • z przodu obudowy: 1x USB 3.2, 1x USB 2.0 (z możliwością zarządzania serwerem), zewnętrzny dedykowany port diagnostyczny, możliwość instalacji portu VGA. • z tyłu obudowy: 2x USB 3.2, 1x USB 2.0 1x VGA, 1x RJ-45 do zarządzania serwerem. Możliwość instalacji portu DB9. • wewnątrz obudowy: 1x USB 3.2. Wszystkie tylne porty USB, port RJ-45 służący do zarządzania, tylny port VGA, wewnętrzny port USB, wewnętrzny port na kartę Micro SD powinny być umieszczone na osobnej dedykowanej płytce I/O, którą łączy się bezpośrednio z płytą główną serwera.
Chłodzenie	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1.
Zarządzanie	Możliwość instalacji zintegrowanego panelu LCD umożliwiającego wyświetlenie poniższych informacji:

	<ul style="list-style-type: none"> • aktywne ostrzeżenia; • Status serwera; • Typ oraz model serwera, numer seryjny; • Wersje oprogramowania UEFI oraz modułu zarządzania; • Informacje nt. modułu zarządzania: nazwa hosta, adres MAC, adres IP, adres DNS; • Dane środowiskowe: temperaturę procesora, poziom napięcia wejściowego, poziom zużycia energii; • Aktywne sesje połączeniowe do interfejsu zarządzania. <p>Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania, który musi być umieszczony na osobnej dedykowanej płycie I/O (wspomnianej w sekcji Dodatkowe Porty). Płyta I/O musi posiadać swój własny min. 2 rdzeniowy procesor o taktowaniu min. 1.2GHz.</p> <ul style="list-style-type: none"> • Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna). • Pozyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres IP karty zarządzającej, użycie CPU, użycie pamięci oraz komponentów I/O, lokalizacja. • Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów. • Logowanie zdarzeń związanych z utrzymaniem systemu jak upgradefirmware, zmiana/installacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń. • Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3. • Update systemowego firmware. • Monitoring i możliwość ograniczenia poboru prądu. • Zdalne włączanie/wyłączenie/restart. • Zapis video zdalnych sesji. • Podmontowanie lokalnych mediów z wykorzystaniem Java Client. • Przekierowanie konsoli szeregowej przez IPMI. • Zrzut ekranu w momencie zawieszenia systemu. • Możliwość przejęcia zdalnego ekranu. • Możliwość zdalnej instalacji systemu operacyjnego. • Alerty Syslog. • Przekierowanie konsoli szeregowej przez SSH. • Wyświetlanie danych aktualnych i historycznych dla użycia energii oraz temperatury serwera. • Możliwość mapowania obrazów ISO z lokalnego dysku operatora. • Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS. • Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę.
--	--

	<ul style="list-style-type: none"> • Wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API. • Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzająca) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego. • Kontroler zarządzania musi posiadać 4Gb wewnętrznej pamięci (dopuszcza się zastosowanie karty Micro SD w celu uzyskania tej pojemności). Pamięć kontrolera zarządzania musi pełnić funkcję RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware. • Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot'u. • Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami. • Możliwość monitorowania i zarządzania grupą serwerów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200. <p>Wraz z serwerem powinno zostać dostarczone dodatkowe oprogramowanie zarządzające umożliwiające:</p> <ul style="list-style-type: none"> - zarządzanie infrastrukturą serwerów i storage bez udziału dedykowanego agenta; - przedstawianie graficznej reprezentacji zarządzanych urządzeń; - możliwość skalowania do minimum 1000 urządzeń; - obsługę szyfrowanej komunikacji z zarządzanymi urządzeniami, wsparcie dla NIST 800-131A oraz FIPS 140-2; - wsparcie dla certyfikatów SSL tzw. self-signed oraz zewnętrznych; - udostępnianie szybkiego podgląd stanu środowiska; - udostępnianie podsumowania stanu dla każdego urządzenia; - tworzenie alertów przy zmianie stanu urządzenia; - monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii; - konsola zarządzania oparta o HTML 5; - dostępność konsoli monitorującej na urządzeniach przenośnych ze wsparciem dla systemu Android oraz iOS, aplikacja musi umożliwiać włączenie wyłączenie oraz restart urządzenia, musi również mieć możliwość aktywowania diody lokacyjnej na urządzeniu; - automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja; - możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o
--	--

	<p>repozytorium lokalne jak i zdalne dostępne na stronie producenta oferowanego rozwiązania;</p> <ul style="list-style-type: none"> - definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzań; - definiowanie roli użytkowników oprogramowania; - obsługa REST API oraz Windows PowerShell; - obsługa SNMP, SYSLOG, Email Forwarding; - autentykacja użytkowników: centralna (możliwość definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z MS AD oraz obsługa single sign on oraz SAML; - obsługa tzw. ForwardSecrecy w komunikacji z zarządzanymi urządzeniami; - przedstawianie historycznych aktywności użytkowników; - blokowanie możliwości podłączenia innego systemu zarządzania do urządzeń zarządzanych; - tworzenie dziennika zdarzeń ukończonych sukcesem lub bledem, oraz zdarzeń będących w trakcie. Możliwość definiowania filtrów wyświetlanych zdarzeń z dziennika. Możliwość eksportu dziennika zdarzeń do pliku csv; - Obsługa NTP; - przesyłanie alertów do konsoli firm trzecich; - tworzenie wzorców konfiguracji zarządzanych urządzeń (definiowanie przez konsole albo kopiowanie konfiguracji z już zaimplementowanych urządzeń); - instalowanie systemów operacyjnych oraz wirtualizatorów VMware i Hyper-V. Wymagana jest integracja konsoli zarządzania z konsolą wirtualizatora tak, aby zarządzanie środowiskiem sprzętowym mogło odbywać się z konsoli wirtualizatora. Wymaga się możliwości instalacji systemu na przynajmniej 20 nodach jednocześnie. - możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta dla określonych zdarzeń wraz z przesyłem plików diagnostycznych. <p>Producent serwera ponadto powinien mieć w swojej ofercie narzędzia integrujące zarządzanie infrastrukturą z następującymi produktami: VMware, vCenter, Microsoft AdminCenter, Microsoft SystemCenter, RedHat CloudForms, Splunk.</p>
Funkcje zabezpieczeń	Możliwość instalacji czujnika otwarcia obudowy zintegrowanego z modułem zarządzania serwerem, hasło włączania, hasło administratora, moduł RoT (umieszczony na dedykowanej płytce I/O wspomnianej w sekcji Dodatkowe porty) wspierający TPM2.0 oraz Platform Firmware Resiliency (PFR). Wymagana możliwość zainstalowania przedniego panelu zabezpieczającego zamykanego na klucz.
Urządzenia hot swap	Dyski twarde, zasilacze, wentylatory.
Diagnostyka	Możliwość przewidywania awarii dla procesorów, regulatorów

	<p>napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID.</p> <p>Możliwość użycia aplikacji mobilnej na telefonie, do przeglądania awarii, konfiguracji i włączenia/wyłączenia serwera.</p>
Systemy operacyjne	Microsoft Windows Server 2019, 2022; Red Hat Enterprise Linux 8.6, 8.7, 9.0, 9.1, SUSE Linux Enterprise Server 15 SP4 oraz 15 Xen SP4; VMware vSphere (ESXi) 7.0 U3, ESXI 8.0; Ubuntu 22.04 LTS
Waga	maximum: 38.8kg
Gwarancja	<p>60 miesięcy gwarancji producenta z oknem serwisowym 24x7. Czas reakcji serwisu – 4 godziny. Uszkodzone nośniki danych pozostają własnością Zamawiającego. Możliwość wykupienia dodatkowego wsparcia, świadczonego przez producenta, z gwarantowanym czasem naprawy w ciągu 6 godzin. W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie Diagnostyka wymagane jest dostarczenie serwera nadmiarowego, mogącego zastąpić funkcjonalnie jak i wydajnościowo wymagane powyżej maszyny. Wszystkie komponenty serwera powinny być sygnowane i zoptymalizowane do użycia przez producenta serwera.</p> <p>Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu złożenia na wezwanie Zamawiającego oświadczenia, że w przypadku wystąpienia awarii nośnika danych w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony nośnik danych pozostaje u Zamawiającego. Dokument musi być oznaczony nazwą i numerem postępowania.</p> <p>Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych lub posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy złożyć na wezwanie Zamawiającego przed przystąpieniem do wykonywania Usług serwisowych. Dokument musi być oznaczony nazwą i numerem postępowania</p> <p>Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.</p> <p>Serwer musi być wyprodukowany zgodnie z normą ISO-9001– dokument należy dołączyć do oferty.</p> <p>Serwer musi posiadać deklaracja CE - dokument należy dołączyć do oferty.</p>
Macierz wydajnościowa – 2 sztuki	
Wymagania	1. Zamówienie dotyczy dostarczenia systemu pamięci masowej składającego się z pojedynczej macierzy. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych połączonych przełącznikami SAN lub tak zwanym

	<p>wirtualizatorem w sieci SAN.</p> <ol style="list-style-type: none">2. Oferowane urządzenie musi być rozwiązaniem kompletnym, pochodzącym od jednego producenta, dostępne w ofercie przed ukazaniem się niniejszego postępowania.3. Macierze i ich elementy składowe zostaną zainstalowane w posiadanych przez Zamawiającego szafach zgodnych ze standardem typu Rack 19”.4. Kompletna pojedyncza macierz nie może przekroczyć wysokości 2U.5. Macierz dyskowa musi być wyposażona w co najmniej jedną parę redundantnych kontrolerów pracujących w trybie active-active.6. Ze względu na wydajność i wielowątkowość pracy wymagane jest, aby każdy kontroler macierzy wyposażony był w co najmniej 12 rdzeni procesora. Dopuszczalna jest kombinacja kilku procesorów dająca w sumie wyżej wymienioną ilość rdzeni.7. Wymagane jest, aby każdy kontroler oferowanej macierzy dyskowej wyposażony był w co najmniej 384 GB natywnej pamięci cache. Nie dopuszcza się rozwiązań gdzie wymagana ilość pamięci cache realizowana jest przez rozszerzenia na dyskach flash/SSD.8. Macierz dyskowa powinna posiadać funkcjonalność partycjonowania pamięci cache. Jeżeli funkcjonalność taka wymaga licencji to należy taką licencję dostarczyć.9. Macierz musi być wyposażona w dwa redundantne zasilacze.10. W przypadku awarii zasilania dane nie zapisane na dyskach, przechowywane w pamięci cache muszą być zabezpieczone metodą trwałego zapisu na dedykowany do tego celu dysk lub nieulotną pamięć podręczną.11. Oferowana macierz dyskowa musi mieć możliwość obsługi połączeń do systemów klienckich o prędkościach i protokołach co najmniej:<ol style="list-style-type: none">a. 16Gbps FC,b. 32Gbps FC,c. 10Gbps iSCSId. 25Gbps iSCSI12. Oferowana macierz musi być macierzą blokową i wykonywać operacje I/O na poziomie bloków danych. Nie dopuszcza się rozwiązania w którym blokowe wolumeny macierzy emulowane są w oparciu o wewnętrzny system plików proponowanego rozwiązania.13. Oferowana macierz dyskowa musi być wyposażona w co najmniej 8 portów FC o prędkości 16 Gbps z możliwością rozbudowy do co najmniej 24 portów FC.14. Macierz powinna umożliwiać konfigurację replikacji synchronicznej i asynchronicznej. Jeżeli taka funkcjonalność jest dodatkowo licencjonowana, nie wymaga się dostarczenia takiej licencji w niniejszym postępowaniu.15. Macierz musi umożliwiać w przyszłości połączenie dwóch
--	--

	<p>macierzy w klastrach, w którym obydwie macierze służą do jednoczesnego odczytu i zapisu danych dla każdego z wolumenów (klastr typu active-active), bez konieczności zakupu dodatkowych urządzeń. Wolumen logiczny dla takiego klastra powinien mieć swoją prezentację na obydwu macierzach. Jeżeli taka funkcjonalność jest dodatkowo licencjonowana, nie wymaga się dostarczenia takiej licencji w niniejszym postępowaniu,</p> <p>16. Wymagane jest, aby macierz dyskowa wspierała różne poziomy zabezpieczeń RAID w tym, co najmniej RAID 1, RAID-5, RAID-6.</p> <p>17. Macierz musi obsługiwać dyski typu: SSD NVMe, SSD, SAS 10k, NL-SAS 7,2k</p> <p>18. Macierz musi umożliwiać rozbudowę do co najmniej 500 dysków.</p> <p>19. Macierz musi być skalowalna do co najmniej 3PB przestrzeni na wewnętrznych dyskach. Poprzez rozbudowę rozumie się dołączenie do macierzy dyskowej kolejnych półek dyskowych producenta macierzy. Wśród dostępnych opcji rozbudowy wymaga się możliwości zastosowania półek gęstego upakowania umożliwiających instalację co najmniej 15 dysków na każde 1U wysokości półki. Wymaga się dostarczenia licencji na pełną wartość obsługiwaną przestrzeni dyskowej.</p> <p>20. Oferowana macierz powinna posiadać możliwość zdefiniowania i udostępnienia serwerom co najmniej 16 tysięcy wolumenów logicznych bez konieczności dokupienia i instalacji dodatkowych licencji.</p> <p>21. Macierz dyskowa powinna umożliwiać utworzenie wolumenu logicznego o rozmiarze co najmniej 60TB.</p> <p>22. Macierz powinna posiadać możliwość definiowania wirtualnych wolumenów logicznych, których pojemność może być większa od rzeczywistej przestrzeni dyskowej skonfigurowanej w obrębie puli dysków twardej („thinprovisioning”). Funkcjonalność „thinprovisioning” powinna być dostarczona wraz z oferowaną macierzą z licencją na nieograniczoną pojemność dyskową. Umożliwiać wystawienie cienkich wolumenów o łącznej pojemności 4.4 PB.</p> <p>23. Przestrzeń proponowanej macierzy dyskowej musi wynosić co najmniej 20TB bez stosowania mechanizmów redukcji (kompresji i/lub deduplikacji), być zbudowana z dysków SSD NVMe, zabezpieczona poziomem RAID gwarantującym dostęp do danych w przypadku awarii dwóch dysków w grupie. Dodatkowo wymaga się dostarczenia w ramach oferowanej konfiguracji dysków typu „hot-spare” dla każdego typu zaofertowanych dysków.</p> <p>24. Macierz musi obsługiwać rozkładanie danych w oparciu o architekturę trzy poziomowego tieringu. Tiering danych musi mieć możliwość zbudowania puli dyskowej w oparciu o warstwy dysków: flash/SSD, SAS, NL-SAS. Jeżeli ta funkcjonalność wymaga licencji to należy ją dostarczyć na</p>
--	--

	<p>pełną przestrzeń wewnętrzną obsługiwaną przez macierz.</p> <p>25. Tiering danych musi być zaimplementowany w kontrolerach macierzy dyskowej i musi posiadać możliwość dynamicznego i automatycznego relokowania fragmentów wolumenów logicznych pomiędzy co najmniej dwoma różnymi klasami pamięci masowej („auto tiering”). Administrator musi mieć możliwość wyboru polityki definiującej warstwę, na którą zapisywane są dane w pierwszej kolejności. Dane z warstwy niższej powinny być promowane do warstwy zbudowanej w oparciu o dyski flash/SSD w sposób natychmiastowy, bez konieczności oczekiwania na zakończenie cyklu monitorowania. Funkcjonalność ta powinna być dostarczona wraz z oferowaną macierzą z licencją na nieograniczoną pojemność dyskową.</p> <p>26. Macierz powinna posiadać możliwość wykonywania pełnych kopii typu klon oraz Snapshotów (migawek) co najmniej 1000 per LUN, które mogą być montowane do dowolnego hosta w trybie zapis / odczyt i pozwalać na:</p> <ul style="list-style-type: none"> a. wykonywanie co najmniej 3 kopii pełnych dla pojedynczego wolumenu źródłowego. b. re-synchronizację danych pomiędzy wolumenami źródłowym i kopią. Podczas wykonywania re-synchronizacji pomiędzy wolumenami kopiowane powinny być tylko dane różnicowe. c. funkcjonalność ta powinna być dostarczona z licencją na nieograniczoną pojemność dyskową oraz nieograniczoną ilość wolumenów. <p>27. Macierz powinna posiadać możliwość migracji całych wolumenów pomiędzy różnymi wolumenami wewnątrz macierzy. Migracja powinna odbywać się w sposób przeźroczysty dla aplikacji (online). Funkcjonalność ta powinna być dostarczona wraz z oferowaną macierzą z licencją na nieograniczoną pojemność dyskową.</p> <p>28. Macierz musi posiadać oprogramowanie do zarządzania, pozwalające na co najmniej:</p> <ul style="list-style-type: none"> a. Tworzenie i nazywanie wolumenów logicznych LUN; b. Mapowanie wolumenów logicznych do serwerów; c. Monitorowanie wykorzystywanej przestrzeni, efektywnej i surowej (RAW) macierzy; d. Tworzenie raportów z konfiguracji macierzy dyskowej; e. Zarządzanie macierzą za pomocą CLI i możliwości tworzenia skryptów z wykorzystaniem komend; f. Zarządzanie wieloma macierzami jednego producenta z jednej konsoli graficznej. <p>29. Należy dostarczyć oprogramowanie pozwalające na całodobowe monitorowanie stanu macierzy i automatyczne informowanie administratorów Zamawiającego o wystąpieniu ewentualnej awarii macierzy. Jeżeli ta funkcjonalność wymaga licencji to należy ją dostarczyć.</p> <p>30. Macierz musi być fabrycznie nowa i pochodzić z oficjalnego kanału dystrybucyjnego producenta w Polsce.</p>
--	--

	<p>31. Macierz powinna posiadać wsparcie producenta na okres 60 miesięcy gwarancji producenta z oknem serwisowym 24x7. Czas reakcji serwisu – 4 godziny. Uszkodzone nośniki danych pozostają własnością Zamawiającego. Możliwość wykupienia dodatkowego wsparcia, świadczonego przez producenta, z gwarantowanym czasem naprawy w ciągu 6 godzin.</p> <p>32. Dostawca musi zagwarantować i potwierdzić, że posiada wymaganą wiedzę i umiejętności do wykonania instalacji macierzy oraz świadczenia serwisu w miejscu jej zainstalowania.</p>
<p>Oprogramowanie do synchronizacji i bezpiecznego udostępniania danych</p>	<p>1. Rozwiązanie musi pozwalać na współdzielenie plików pomiędzy uczestnikami projektu, pracownikami wewnątrz organizacji (w ramach wykorzystywanego katalogu usług Active Directory) oraz na zewnątrz organizacji (dla podmiotów współpracujących, kontraktorów, firm zewnętrznych).</p> <ul style="list-style-type: none"> • Współdzielenie plików musi być realizowane poprzez udostępnienie linku do pliku lub katalogu. • Definicja linku powinna zawierać co najmniej: <ul style="list-style-type: none"> - datę, po której link przestanie być dostępny, - typu linku: prywatny (dostępny tylko wewnątrz organizacji) lub publiczny (dostępny dla wszystkich), - dodatkowe hasło, które musi być przekazane w sposób niezależny od samego linku. • W przypadku udostępniania katalogu musi istnieć dodatkowa możliwość definiowania uprawnień dla odbiorcy, w tym co najmniej „odczyt i zapis” oraz „tylko odczyt”. • Musi istnieć możliwość zarządzania linkami, w tym co najmniej: zmiana daty ważności linku, kasowanie linku, generowanie hasła do linku. • Musi istnieć możliwość tworzenia linków stałych – bez definicji daty ich ważności. • Użytkownik powinien być powiadamiany o pobraniu współdzielonego pliku oraz o zapisaniu pliku w udostępnionym katalogu. • Musi istnieć możliwość tworzenia folderów do pracy grupowej. Przestrzeń folderów do pracy grupowej nie powinna wykorzystywać przyznanego przez administratora limitu przestrzeni (quota) dla pozostałych plików. • Definicja folderu współdzielonego wewnątrz organizacji oraz folderu pracy grupowej musi zawierać: <ul style="list-style-type: none"> - możliwość opuszczenia folderu (rezygnacja z dostępu do folderu), - możliwość wyłączenia współdzielenia, - możliwość dodawania i usuwania użytkowników folderu, - możliwość definiowania uprawnień dla użytkowników folderu. <p>2. Rozwiązanie musi pozwalać na synchronizację plików pomiędzy różnymi urządzeniami.</p> <ul style="list-style-type: none"> • Muszą być wspierane co najmniej następujące systemy operacyjne: Windows, OS X, Android, iOS.

	<ul style="list-style-type: none"> • Użytkownik powinien mieć możliwość zatrzymania i wznowienia synchronizacji plików. • Użytkownik musi mieć możliwość rejestracji w ramach swojego konta wielu różnych urządzeń. • Rozwiązanie musi umożliwiać zdalne usunięcie danych z urządzenia, które zostało skradzione lub zagubione. • Instalacja klienta systemu na urządzeniu mobilnym użytkownika musi wymagać włączenia mechanizmów bezpiecznego logowania do urządzenia (co najmniej 6 cyfrowy PIN, logowanie biometryczne). • Instalacja klienta systemu na urządzeniu użytkownika musi być realizowana bezpośrednio przez użytkownika, bez konieczności ingerencji działu IT. Administratorzy IT powinni mieć natomiast możliwość definicji, ile i z jakich urządzeń klienckich może korzystać użytkownik. <p>3. Użytkownik korzystający z funkcjonalności współdzielenia i synchronizacji plików musi mieć dostęp do swoich plików w następujący sposób:</p> <ul style="list-style-type: none"> • w postaci katalogu w systemie plików na swoim komputerze (on-line i off-line), • w aplikacji mobilnej na swoim smartfonie i tablecie (on-line i off-line), • w przeglądarce internetowej (on-line). <p>4. Wszystkie współdzielone i synchronizowane pliki muszą być przechowywane i zabezpieczone w dedykowanej logicznej partycji dostarczanej macierzy obiektowej. Dopuszcza się macierz obiektową w wersji fizycznej jak i wirtualnej.</p> <p>5. Wszystkie współdzielone i synchronizowane pliki powinny być wersjonowane. Użytkownik musi mieć możliwość przeglądania historii wersji oraz odzyskiwania wersji plików. Administrator IT musi mieć możliwość skonfigurowania: ilości ostatnich wersji pliku oraz okresu po jakim wersje mają być nieodwracalnie kasowane z systemu.</p> <p>6. Użytkownik musi mieć możliwość samodzielnego (bez udziału Administratora IT) odzyskiwania skasowanych plików. Rozwiązanie musi umożliwiać definiowanie okresu przechowywania skasowanych plików.</p> <p>7. Funkcjonalność współdzielenia i synchronizacji musi być realizowana za pomocą komponentów zainstalowanych w centrum przetwarzania Zamawiającego. Zamawiający nie dopuszcza rozwiązań, w których jakkolwiek element rozwiązania jest zainstalowany i dostępny w chmurze publicznej.</p> <p>8. Wskazani Administratorzy IT muszą mieć możliwość przeprowadzenia inspekcji aktywności zarejestrowanych użytkowników w zakresie współdzielonych i udostępnionych plików, w tym możliwość pobrania i usunięcia niepożądanych treści.</p> <p>9. Zamawiający wymaga, aby funkcjonalność węzłów</p>
--	--

	<p>synchronizacji i współdzielenia plików realizowana była poprzez rozwiązania programowe uruchamiane na węzłach w warstwie wirtualizacyjnej (VMware, Hyper-V, KVM i inne) zapewniające architekturę HA dla węzłów (przełączenie pomiędzy podstawową a zapasową serwerownią Zamawiającego).</p> <p>10. Musi istnieć możliwość integracji zasobów plikowych przechowywanych na dyskach sieciowych w ramach interfejsu użytkownika do współdzielenia i synchronizacji plików. To oznacza, że użytkownik ten musi mieć możliwość dostępu do swoich zasobów plikowych przechowywanych na dyskach sieciowych zarówno w przeglądarce internetowej jak i w aplikacji mobilnej systemu współdzielenia i synchronizacji plików.</p> <p>11. Rozwiązanie powinno posiadać możliwość zarządzania co najmniej poprzez graficzny interfejs użytkownika oraz poprzez API.</p> <p>12. Rozwiązanie musi posiadać możliwość integracji z Microsoft Office Online Server i zapewniać równoległą pracę na współdzielonym dokumencie w formacie Microsoft Word, Excel i Power Point uprawnionym użytkownikom a także podgląd plików PDF.</p>
Przełącznik SAN z niezbędnym okablowaniem i wkładkami FC – 2 sztuki	
Obudowa	Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U wraz z kompletem odpowiednich szyn mocujących dedykowanych przez producenta przełącznika.
Technologia	<p>Przełącznik FC musi być wykonany w technologii FC minimum 32 Gb/s i zapewniać możliwość pracy portów FC z prędkościami 32, 16, 8, 4 Gb/s w zależności od rodzaju zastosowanych wkładek SFP.</p> <p>W przypadku obsadzenia portu FC za pomocą wkładki SFP 16Gb/s przełącznik musi umożliwiać pracę tego portu z prędkością 16, 8, 4 Gbs, przy czym wybór prędkości musi być możliwy w trybie autonegociacji.</p> <p>Przełącznik FC musi mieć możliwość instalacji wkładek SFP umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 25km z prędkością 16Gb/s. Jeśli powyższa funkcjonalność wymaga licencji, nie wymaga się jej w momencie dostawy przełącznika.</p>
Porty	Przełącznik FC musi być wyposażony, w co najmniej 8 aktywnych portów FC obsadzone wkładkami SFP 16Gb/s krótkiego zasięgu. Rodzaj obsługiwanych portów: E, D, M oraz F.
Przepustowość	<p>Architektura non-blocking pozwalająca na pracę wszystkich portów przełącznika równocześnie z pełną prędkością 32Gb/s lub 16Gb/s w zależności do zastosowanych wkładek FC.</p> <p>Całkowita przepustowość przełącznika FC musi wynosić minimum 768Gb/s. Opóźnienie przy przesyłaniu ramek FC między dowolnymi portami przełącznika nie większe niż 1μs.</p>

Funkcjonalność	<p>Przełącznik FC musi mieć możliwość agregacji połączeń ISL między dwoma przełącznikami z przynajmniej ośmiu linków. Połączenie zagregowane musi być zrealizowane na poziomie ramek FC. Jeśli do aktywacji tej funkcjonalności wymagana jest dedykowana licencja, nie wymaga się jej w momencie dostawy. Przełącznik FC musi wspierać następujące mechanizmy zwiększające poziom bezpieczeństwa:</p> <ul style="list-style-type: none"> • szyfrowanie połączenia z konsolą administracyjną, wsparcie dla SSH, • definiowanie wielu kont administratorów z możliwością ograniczenia ich uprawnień za pomocą mechanizmu tzw. RBAC (Role Based Access Control), • definiowane kont administratorów w środowisku RADIUS, Active Directory, LDAP, TACACS+, • szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS, • obsługa SNMP, • obsługa protokołów SCP oraz SFTP.
Zarządzanie i konfiguracja	<p>Możliwość zarządzania poprzez konsole graficzną oraz tryb tekstowy CLI. Interfejsy: zintegrowany port Ethernet, RS232 oraz port USB na potrzeby przenoszenia plików firmware, plików konfiguracji, plików log.</p>
Gwarancja i wsparcie	<p>60 miesięcy gwarancji producenta z oknem serwisowym 24x7. Czas reakcji serwisu – 4 godziny. Możliwość zgłaszania awarii poprzez linię telefoniczną producenta lub firmy serwisującej. Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych lub posiadać autoryzację producenta urządzeń – dokumenty potwierdzające należy złożyć na wezwanie Zamawiającego przed przystąpieniem do wykonywania Usług serwisowych. Dokument musi być oznaczony nazwą i numerem postępowania</p> <p>Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.</p>
<p>Oprogramowanie serwerowe – 8 sztuk Typu Microsoft Windows Server Standard</p>	
Kryteria równoważności dla oprogramowania	<ol style="list-style-type: none"> 1. System operacyjny przeznaczony dla serwerów z graficznym interfejsem użytkownika umożliwiający jego obsługę przy pomocy klawiatury i myszy. 2. Interfejs użytkownika systemu operacyjnego musi pozwalać na zmianę języka interfejsu. 3. Licencja na system musi umożliwiać wykonywanie aktualizacji i otrzymywanie poprawek bezpieczeństwa systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 4. System musi posiadać wbudowaną zaporę sieciową (firewall) dla połączeń przychodzący i wychodzących z systemu. 5. System musi posiadać wbudowane mechanizmy ochrony

	<p>przeciw złośliwemu oprogramowaniu oraz antywirusa działającego w trybie rzeczywistym wraz z bezpłatnymi aktualizacjami.</p> <p>6. System musi posiadać wsparcie dla urządzeń peryferyjnych typu drukarki, urządzenia USB, urządzenia Plug&Play</p> <p>7. System musi posiadać możliwość zarządzania konfiguracją poprzez polityki grupowe - reguł definiujących wymagany poziom bezpieczeństwa lub funkcjonalność systemu</p> <p>8. System musi posiadać mechanizmy logowania do domeny w oparciu o login i hasło lub karty z certyfikatami.</p> <p>9. System musi posiadać natywne wsparcie dla środowiska .NET Framework 4.x.</p> <p>10. System musi posiadać wbudowane mechanizmy szyfrowania dysków podłączonych do systemu z możliwością przechowywania certyfikatów w module TPM</p> <p>11. System musi posiadać identyfikację sieci do której podłączony jest system operacyjny i automatyczne stosowanie na tej podstawie reguł bezpieczeństwa.</p> <p>12. Licencja: licencja bezterminowa, na serwerowy system operacyjny obejmująca konfigurację nie niższej niż 1 procesor 16-rdzeniowy per serwer.</p> <p>13. Oprogramowanie musi charakteryzować się cechami wskazanymi poniżej:</p> <p>13.1. Oferowane rozwiązanie musi uprawniać do instalacji\uruchomienia minimum 2 środowisk gości działających pod kontrolą systemu operacyjnego z rodziny MS Windows.</p> <p>13.2. Oferowane rozwiązanie musi pozwalać na wykorzystanie przez hosta minimum 64 procesorów logicznych, 2 TB pamięci RAM.</p> <p>13.3. Oferowane rozwiązanie musi pozwalać na wykorzystywanie przez gościa minimum 32 procesorów wirtualnych, 1 TB pamięci RAM, dysku o pojemności do 2 TB.</p> <p>13.4. Oferowane rozwiązanie musi posiadać możliwość budowania klastrów niezawodnościowych składających się 16 węzłów (odpowiednik funkcjonalności FailoverClusters).</p> <p>13.5. Oferowane rozwiązanie musi posiadać możliwość federowania klastrów typu niezawodnościowego (FailoverClusters) w zespół klastrów z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu (odpowiednik funkcjonalności Cluster Set).</p> <p>13.6. Oferowane rozwiązanie musi posiadać możliwość narzucania wieloelementowej dynamicznej kontroli dostępu</p>
--	---

	<p>dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.</p> <p>13.7. Oferowane równoważne rozwiązanie musi posiadać możliwość automatycznej aktualizacji w modelu „rolling update”:</p> <p>13.7.1. w oparciu o poprawki publikowane przez producenta w sieci Internet,</p> <p>13.7.2. z możliwością lokalnej dystrybucji poprawek zatwierdzonych przez administratora rozwiązania, bez połączenia z siecią Internet.</p>
<p>Oprogramowanie bazodanowe – 2 sztuki Licencji Oracle SE2 na procesor lub równoważna.</p>	
<p>Wymagania</p>	<ol style="list-style-type: none"> 1. Dostępność oprogramowania na współczesne 64-bitowe platformy Unix (HP-UX dla procesorów Itanium, Solaris dla procesorów SPARC i Intel/AMD, IBM AIX dla procesorów POWER, Intel/AMD Linux, MS Windows). Identyczna funkcjonalność serwera bazy danych na ww. platformach 2. Dostarczone licencje nie mogą ograniczać liczby użytkowników końcowych korzystających z oprogramowania ani liczby przetwarzanych lub przechowywanych dokumentów, plików, rekordów, żądań, wykorzystywanych systemów dziedzinowych etc. Licencje nie mogą być ograniczone czasowo. 3. Proponowany zestaw licencji powinien być jednorodny. Wymagana jest dostawa oprogramowania certyfikowanego pod względem zgodności ze sobą. Wymaganie obejmuje: <ul style="list-style-type: none"> - Oprogramowanie bazy danych ze względu na zgodność z systemem operacyjnym oraz platformą sprzętową, - Systemy operacyjne używane do uruchamiania serwerów bazy danych ze względu na zgodność z platformą sprzętową. 4. Dostępność narzędzi migracji baz danych pomiędzy platformami na poziomie fizycznym (kopiowanie / konwersja plików danych) oraz logicznym (narzędzia eksportu / importu). 5. Oprogramowanie klienckie, za pomocą którego można łączyć się do bazy danych musi być dostępne na wielu platformach systemowo-sprzętowych (minimalny zakres platform taki jak dla oprogramowania serwera bazy danych) 6. Wsparcie protokołu XA. 7. Wsparcie standardu JDBC 3.0. 8. Zgodność ze standardem ANSI/ISO SQL 2003 lub nowszym. 9. Wbudowana obsługa wyrażeń regularnych zgodna ze standardem POSIX dostępna z poziomu języka SQL jak i procedur/funkcji składowanych w bazie danych. 10. RDBMS musi zapewniać niezależność platformy systemowej dla oprogramowania klienckiego od platformy systemowej bazy danych. 11. RDBMS musi zapewniać przetwarzanie transakcyjne wg reguł ACID z zachowaniem spójności i maksymalnego

	<p>możliwego stopnia współbieżności. Mechanizm izolowania transakcji musi pozwalać na spójny odczyt modyfikowanego obszaru danych bez wprowadzania blokad, spójny odczyt nie może blokować możliwości wykonywania zmian.</p> <p>12. RDBMS musi posiadać możliwość zagnieżdżania transakcji – możliwość uruchomienia niezależnej transakcji wewnątrz transakcji nadrzędnej.</p> <p>13. Dostępność nieblokującego poziomu izolowania transakcji „tylko do odczytu” (Read Only) pozwalający na uzyskanie w wielu kolejnych następujących po sobie zapytaniach rezultatów odzwierciedlających stan danych z chwili rozpoczęcia ww. transakcji.</p> <p>14. Dostępność poziomu serializowanego poziomu izolowania transakcji (Serializable).</p> <p>15. Możliwość zmiany domyślnego trybu izolowania transakcji (Read Committed) na inny (Read Only, Serializable) za pomocą komend serwera bazy danych.</p> <p>16. Wsparcie dla wielu ustawień narodowych i wielu zestawów znaków (włącznie z Unicode) zarówno po stronie serwera bazy danych jak i oprogramowania klienckiego. Wsparcie dla polskich stron kodowych – ISO-8859-2, MS Windows CodePage 1250 oraz PC 852. Automatyczna konwersja znaków pomiędzy różnymi ustawieniami stron kodowych po stronie klienta i serwera bazy danych.</p> <p>17. Możliwość migracji bazy danych utrzymujących dane znakowe w 8-bitowej stronie kodowej do Unicode.</p> <p>18. Możliwość definiowania w przestrzeni danych (plików) dla danych użytkownika obszarów o innym niż domyślny rozmiarze bloku.</p> <p>19. Możliwość bez dodatkowych ograniczeń przechowywania wierszy, których rozmiar przekracza rozmiar bloku bazy danych.</p> <p>20. Możliwość budowania indeksów o strukturze B-drzewa. Baza danych powinna umożliwiać założenie indeksu jednej lub większej liczbie kolumn tabeli, przy czym ograniczenie liczby kolumn na których założony jest 1 indeks nie powinno być mniejsze niż 16.</p> <p>21. Możliwość budowania widoków zmaterializowanych odzwierciedlających stan danych zdefiniowanych przez zapytanie SQL. Widok zmaterializowany przechowuje rezultat zapytania, którego aktualizacja odbywa się w jednej z dostępnych strategii – na żądanie, okresowo bądź po każdym zatwierdzeniu transakcji modyfikującej tabelę, na której oparty jest widok zmaterializowany.</p> <p>22. Możliwość szybkiego odświeżania danych w widoku zmaterializowanym na podstawie mechanizmu identyfikacji zmian w danych źródłowych.</p> <p>23. Brak formalnych ograniczeń na liczbę tabel i indeksów w bazie danych oraz na ich rozmiar (liczbę wierszy).</p> <p>24. Kosztowy model optymalizacji instrukcji SQL.</p>
--	--

	<p>25. Model statystyk optymalizatora kosztowego musi pozwalać na odwzorowanie nierównomierności rozkładu danych (składowanie informacji o rozkładzie wartości występujących w kolumnach za pomocą histogramu bądź porównywalnego funkcjonalnie modelu odwzorowania).</p> <p>26. Możliwość uwzględnienia korelacji wartości występujących w niezależnych kolumnach tabeli w modelu statystyk optymalizatora kosztowego.</p> <p>27. RDBMS powinien umożliwiać wskazywanie optymalizatorowi SQL preferowanych metod optymalizacji na poziomie konfiguracji parametrów pracy serwera bazy danych oraz dla wybranych zapytań. Powinna istnieć możliwość umieszczania wskazówek dla optymalizatora w wybranych instrukcjach SQL.</p> <p>28. Wsparcie dla procedur i funkcji składowanych w bazie danych. Język programowania powinien być językiem proceduralnym, blokowym (umożliwiającym deklarowanie zmiennych wewnątrz bloku), oraz wspierającym obsługę wyjątków. W przypadku, gdy wyjątek nie ma zadeklarowanej obsługi wewnątrz bloku, w razie jego wystąpienia wyjątek powinien być automatycznie propagowany do bloku nadrzędnego bądź wywołującej go jednostki programu.</p> <p>29. Procedury i funkcje składowane powinny mieć możliwość parametryzowania za pomocą parametrów prostych jak i parametrów o typach złożonych, definiowanych przez użytkownika. Funkcje powinny mieć możliwość zwracania rezultatów jako zbioru danych, możliwego do wykorzystania jako źródło danych w instrukcjach SQL (czyli występujących we frazie FROM). Ww. jednostki programowe powinny umożliwiać wywoływanie instrukcji SQL (zapytania, instrukcje DML, DDL), umożliwiać jednoczesne otwarcie wielu tzw. cursorów pobierających paczki danych (wiele wierszy za jednym pobraniem) oraz wspierać mechanizmy transakcyjne (np. zatwierdzanie bądź wycofanie transakcji wewnątrz procedury).</p> <p>30. Możliwość kompilacji procedur składowanych w bazie do postaci kodu binarnego (biblioteki dzielonej).</p> <p>31. Możliwość deklarowania wyzwalaczy (triggerów) na poziomie instrukcji DML (INSERT, UPDATE, DELETE) wykonywanej na tabeli, poziomie każdego wiersza modyfikowanego przez instrukcję DML oraz na poziomie zdarzeń bazy danych (np. próba wykonania instrukcji DML, start serwera, stop serwera, próba zalogowania użytkownika, wystąpienie specyficznego błędu w serwerze). Ponadto mechanizm wyzwalaczy powinien umożliwiać oprogramowanie obsługi instrukcji DML (INSERT, UPDATE, DELETE) wykonywanych na tzw. niemodyfikowalnych widokach (views).</p> <p>32. W przypadku, gdy w wyzwalaczu na poziomie instrukcji DML wystąpi błąd zgłoszony przez motor bazy danych bądź</p>
--	---

	<p>ustawiony wyjątek w kodzie wyzwalacza, wykonywana instrukcja DML musi być automatycznie wycofana przez serwer bazy danych, zaś stan transakcji po wycofaniu musi odzwierciedlać chwilę przed rozpoczęciem instrukcji w której wystąpił ww. błąd lub wyjątek.</p> <p>33. Możliwość wykonania równoczesnych operacji DML (Insert/Update/Delete) na tej samej tabeli .</p> <p>34. Powinna istnieć możliwość autoryzowania użytkowników bazy danych za pomocą rejestru użytkowników założonego w bazie danych bądź mechanizmu zewnętrznego w stosunku do bazy danych.</p> <p>35. Przywileje użytkowników bazy danych powinny być określone za pomocą przywilejów systemowych (np. prawo do połączenia się do bazy danych - czyli utworzenia sesji, prawo do tworzenia tabel itd.) oraz przywilejów dostępu do obiektów aplikacyjnych (np. odczytu / modyfikacji tabeli, wykonania procedury). Baza danych powinna umożliwiać nadawanie ww. przywilejów za pośrednictwem mechanizmu grup użytkowników / ról bazodanowych. W danej chwili użytkownik może mieć aktywny dowolny podzbiór nadanych ról bazodanowych.</p> <p>36. Możliwość wykonywania i katalogowania kopii bezpieczeństwa bezpośrednio przez serwer bazy danych. Możliwość zautomatyzowanego usuwania zbędnych kopii bezpieczeństwa przy zachowaniu odpowiedniej liczby kopii nadmiarowych - stosownie do założonej polityki nadmiarowości backup'ów. Możliwość integracji z powszechnie stosowanymi systemami backupu (Legato, Veritas, Tivoli, itp.). Wykonywanie kopii bezpieczeństwa powinno być możliwe w trybie offline oraz w trybie online(hot backup).</p> <p>37. Odtwarzanie powinno umożliwiać odzyskanie stanu danych z chwili wystąpienia awarii bądź cofnąć stan bazy danych do punktu w czasie. W przypadku odtwarzania do stanu z chwili wystąpienia awarii odtwarzaniu może podlegać cała baza danych bądź pojedyncze pliki danych.</p> <p>38. Motor bazy danych na poziomie wskazanego numeru wersji wydania musi zapewnić wbudowany, własny mechanizm umożliwiający uruchomienia środowiska w konfiguracji klastrowej wykorzystującej dwa węzły jako podstawę architektury rozwiązania</p> <p>39. Licencje motoru bazy danych muszą być dostarczone w ilości 2 sztuk. Zamawiający dopuszcza zakup licencji dedykowanych dla aplikacji AMMS Asseco Poland S.A. (ASFU)</p>
Gwarancja	Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikro kodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.
Wsparcie techniczne producenta	Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

	Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera – należy dołączyć link strony.
--	---

Usługi utrzymaniowe w zakresie infrastruktury Zamawiającego

Zamawiający wymaga świadczenia usług utrzymania dostarczonej infrastruktury IT oraz systemów, przez okres 12 miesięcy licząc od daty podpisania protokołu odbioru końcowego bez uwag, według poniższego zakresu:

- a) przygotowywanie aktualizacji (upgrade) dostarczonego przedmiotu umowy,
- b) wykonanie aktualizacji (upgrade) dostarczonego przedmiotu umowy w oknie serwisowym wyznaczonym przez Zamawiającego,
- c) monitoringu ciągłości działania infrastruktury IT,
- d) usuwania ewentualnych awarii infrastruktury IT,
- e) raportowanie wykonanych prac w cyklu miesięcznym z wyszczególnieniem istotnych zdarzeń zagrażających bezpieczeństwu informatycznemu Zamawiającego.

Usługi będą świadczone w godzinach 8:00-15:00 w dni robocze.