Zamówienie finansowane ze środków budżetu Województwa Śląskiego

Załącznik nr 1.2 do SWZ
AZP/P/25/2025

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

w zakresie pakietu nr 1

Spis treści

1. Wprowadzenie

Wdrożenie zespołu macierzy dyskowych

Zadanie polega na dostawie oraz wdrożeniu macierzy dyskowej z niezbędną infrastrukturą, serwera dedykowanego dla bazy danych oraz zmigrowania i optymalizację danych, w tym baz danych na nowo tworzonym środowisku. Zamawiający obecnie posiada 2 niezależne klastry serwerów HA pracujące na środowisku vsphere firmy Vmware oraz Microsoft Hyper-V.

Zamawiający korzysta z szeregu rozwiązań firmy ASSECO POLAND oraz w zakresie systemów RIS/PACS firmy PIXEL. Zamawiający wymaga przeniesienia z istniejących środowisk wirtualnych łącznie do 30 maszyn wirtualnych o łącznej pojemności 15 tb w tym Zamawiający posiada bazę danych Oracle SE, którą Wykonawca zaktualizuje do najnowszej wersji wraz z dostarczeniem nowej licencji bazy ze wsparciem producenta oraz dokona prac optymalizacyjnych i migracji do nowego środowiska. Dokładny wykaz maszyn do migracji z starego środowiska vSphere Zamawiający przekaże po zawarciu umowy z Wykonawcą

W zakresie systemu wirtualizacji, Zamawiający zamierza wykorzystać najnowszy system wirtualizacji, zapewniony w ramach dostarczanych licencji oprogramowania serwerowego.

Wykonawca przygotuje we własnym zakresie środowisko niezbędne do przeprowadzenia migracji w taki sposób, aby nie wpływało to na bieżące funkcjonowanie szpitala. Wykonawca zapewni niezbędny sprzęt oraz zasoby do prawidłowego przeprowadzenia migracji środowiska. Poniżej przedstawiono plan zadań do wykonania przez wykonawcę:

- Przygotowanie harmonogramu dostaw, instalacji oraz prac wdrożeniowych
- Przygotowanie dokumentacji projektowej DAP
- Aktualizacja oprogramowania mikrokodów (tzw firmware) na posiadanym przez Zamawiającego sprzęcie serwerowym oraz macierzowym (2 serwery Fujitsu oznaczone dalej jako S1 i S2 oraz 3 serwerów DELL PE oznaczonych dalej jako S3, S4, S5 oraz macierzy Hitachi Oznaczonej jako ZD1)
- Rozbudowa istniejących serwerów S1 i S2 o karty FC 32GBPS
- Wykonanie kopii zapasowej całego środowiska
- Uruchomienie środowiska tymczasowego i przeniesienie zasobów maszyn wirtualnych około 30 maszyn na środowisko tymczasowe
- Instalacja i konfiguracja nowego środowiska wirtualizacji oraz systemów operacyjnych, dostarczanych w ramach niniejszego postępowania, na 2 posiadanych przez Zamawiającego serwerach Fujitsu
- Konfiguracja serwerów S1 i S2 do działania jako klaster wysokiej dostępności
- Instalacja, konfiguracja oraz podłączenie nowej macierzy dyskowej, dostarczanej w ramach niniejszego postępowania i udostepnienie zasobów dla nowo powstałego klastra wirtualizacji
- Podłączenie serwerów klastra do struktury sieci SAN
- Migracja maszyn wirtualnych z środowiska tymczasowego wraz z konwersją do plików .vhd/.vhdx i uruchomienie.
- Aktualizacja produkcyjnej bazy danych do najnowszej wersji oraz prace konfiguracyjne i optymalizacyjne
- Testy akceptacyjne
- Przygotowanie dokumentacji powykonawczej

1. Przedmiot Zamówienia będzie realizowany w oparciu o zdefiniowany uprzednio przez Wykonawcę i zaakceptowany Harmonogram wdrożenia, który powinien być uzgodniony i zaakceptowany przez Zamawiającego oraz odpowiednio utrzymywany w toku realizacji Przedmiotu Zamówienia.
2. Wykonawca w Harmonogramie wdrożenia musi uwzględnić w szczególności podział na zadania takie jak projektowanie, dostawy, usługi instalacji/konfiguracji, testowanie, wdrożenie i odbiory.
3. Wykonawca umożliwi Zamawiającemu udział we wszystkich pracach realizowanych przez Wykonawcę w ramach realizacji Przedmiotu Zamówienia (m.in. w czasie projektowania, dostawach, instalacji/budowie, konfiguracji wdrożeniu i testowaniu).
4. Wykonawca zobowiązany jest do udziału w cyklicznych naradach przeglądu prac w siedzibie Zamawiającego. Zamawiający przewiduje częstotliwość narad maksymalnie 1 raz w miesiącu, chyba że nadzwyczajna sytuacja w realizacji przedmiotu umowy wymagała będzie częstszych spotkań.
5. Wykonawca zobowiązany jest przeprowadzić dostawy Przedmiotu Zamówienia w dokładnych terminach i godzinach uzgodnionych z Zamawiającym.
6. W przypadku dostarczania Infrastruktury informatycznej musi być ona oznakowana w taki sposób, aby możliwa była identyfikacja systemowa zarówno produktu jak i producenta, pochodził z oficjalnych kanałów dystrybucji producentów i dostarczony w oryginalnych opakowaniach fabrycznych.
7. Wdrożenie należy rozumieć jako szereg uporządkowanych i zorganizowanych działań mających na celu wykonanie Przedmiotu Zamówienia.
8. Wdrożenie będzie realizowane w ramach powołanych do tego celu struktur organizacyjnych po stronie Wykonawcy.

9. W ramach wdrożenia Wykonawca przygotuje informacje na temat struktury organizacyjnej Zespołu Wykonawcy zajmującej się realizacją Przedmiotu Zamówienia, w ramach której muszą zostać powołane minimum następujące role:
a. Koordynator Projektu ze strony Wykonawcy,
b. Zespół Wdrożeniowy ze strony Wykonawcy.
10. Wdrożenie, z zastrzeżeniami wskazanymi poniżej w punktach muszą realizować osoby wymienione w ofercie Wykonawcy (Wykaz osób), przy czym:
a. Osoby Zespołu Wykonawcy muszą być dyspozycyjne w trakcie wykonywania prac,
b. Wykonawca przekaże Zamawiającemu wykaz numerów telefonów kontaktowych do osób biorących udział w realizacji Przedmiotu Zamówienia po stronie Wykonawcy,
11. Wykonawca zorganizuje prace tak, aby w maksymalnym stopniu nie zakłócać ciągłości funkcjonowania prac u Zamawiającego.
12. Obiekty podlegające inwestycji (obiekty służby zdrowia, w których świadczone są usługi medyczne) są użytkowane w trybie ciągłym w czasie godzin pracy przez cały okres wykonywania Przedmiotu Zamówienia, co może powodować utrudnienia w miejscu prowadzenia prac. Nie ma możliwości całkowitego wyłączenia i zamknięcia w/w obiektów lub ich części na czas realizacji Przedmiotu Zamówienia. Poszczególne prace będą realizowane etapowo, tak aby zachować ciągłość świadczenia usług medycznych.
13. Wykonawca musi uwzględnić, że wszystkie prace wykonywane będą w użytkowanych obiektach przy dużym ruchu pracowników i chorych, tzn. organizacja prac powinna przede wszystkim zapewniać bezpieczeństwo przebywających w oddziałach pracowników i chorych oraz zachowanie ciszy nocnej w godzinach właściwych dla Zamawiającego.

Przygotowanie Dokumentacji
1. W ramach procesu prac Wykonawca opracuje dla Zamawiającego Dokumentację Przedmiotu Zamówienia (zwaną dalej Dokumentacją), która składa się z nw. zakresów:
a) Harmonogram Wdrożenia,
b) Dokumentacja Analizy Przedwdrożeniowej (DAP),
c) Dokumentacja Powykonawcza.
2. Dokumentacja powyższa będzie zawierać bazowe zapisy opisujące budowane rozwiązania, procesy oraz sposób organizacji prac i wdrożenia. Na podstawie zapisów w Dokumentacji będą prowadzone i odbierane poszczególne etapy realizowane w ramach Przedmiotu zamówienia. Dokumenty te wraz ze Specyfikacją Warunków Zamówienia wraz z załącznikami (dalej zwanych SWZ) będą stanowiły podstawę do weryfikacji wdrożenia w trakcie odbiorów.
3. Dokumentacja podlega uzgadnianiu i akceptacji Zamawiającego. Akceptacja Harmonogramu wdrożenia, DAP warunkuje rozpoczęcie prac Wykonawcy.
4. Dokumentacja Analizy Przedwdrożeniowej DAP wraz z Harmonogramem wdrożenia zostaną opracowane w oparciu o wymagania określone w niniejszym SOPZ.

Harmonogram wdrożenia
Wykonawca zobowiązany jest opracować na podstawie SWZ oraz SOPZ szczegółowy harmonogram wdrożenia. Harmonogram należy przedstawić Zamawiającemu w terminie do 7 dni od podpisania Umowy.

Analiza Przedwdrożeniowa
1. Analiza przedwdrożeniowa, którą należy rozumieć jako zakres czynności do wykonania przez Wykonawcę mający na celu analizę środowiska biznesowego i informatycznego Zamawiającego. W wyniku przeprowadzenia Analizy przedwdrożeniowej Wykonawca przedstawi Zamawiającemu Dokumentacje analizy przedwdrożeniowej (zwana dalej DAP), na podstawie, której będzie realizowany organizacyjnie i technicznie Przedmiot Zamówienia. Dokumentacja Analizy Przedwdrożeniowej będzie podlegała uzgodnieniu i akceptacji Zamawiającego.
2. Dokumentacja Analizy Przedwdrożeniowej DAP powinna zawierać w szczególności:

SKŁAD DAP

- wykaz oraz szczegółowy opis i harmonogram budowy środowiska
- architekturę środowiska
- analizę i plan migracji danych oraz opis sposobu migracji danych który posiada Zamawiający
- przygotowanie planu instalacji Infrastruktury serwerowej
- przygotowanie planu instalacji macierzy dyskowych
- jednoznacznie określone założenia integracji z innymi systemami informatycznymi, które posiada Zamawiając
- plan pracy na wszystkie etapy Wdrożenia
- szczegółowe specyfikacje oprogramowania objętego zakresem umowy
- wykaz oraz szczegółowy opis i harmonogram niezbędnych prac konfiguracyjnych
- ustawienia konfiguracyjne urządzeń i oprogramowania
- propozycje scenariuszy testowych uwzgledniających zakres czynności operacyjnych, które należy wykonać w celu potwierdzenia, że wskazane wymagane funkcjonalności zostały prawidłowo skonfigurowane I działające zgodnie z opisami procesów
- harmonogram instruktażu administratorów
INFRASTRUKTURA SERWEROWA
- podział Przedmiotu Zamówienia na Produkty, a następnie ich pogrupowanie w Komponenty
- analizę wymagań Przedmiotu Zamówienia zawierające opis sposobu realizacji wymagań, sposób testowania i odbioru
- karty katalogowe urządzeń potwierdzające spełnienie wymagań
- plan dostaw
- opis instalacji wdrożenia oprogramowania wdrażanego wraz z Infrastrukturą serwerową
- opis modernizacji budowy Infrastruktury serwerowej - jeżeli dotyczy
- lista Komponentów, które będę podlegały osobnym odbiorom – jeżeli dotyczy
- szczegółowy zakres i zawartość pozostałej Dokumentacji

Dokumentacja Powykonawcza

1. Warunkiem dokonania Odbioru Końcowego jest dostarczenie przez Wykonawcę Dokumentacji Powykonawczej obejmującej dokumentację użytkową, techniczną i eksploatacyjną. Dokumentacja Powykonawcza musi być dostarczona w języku polskim, w wersji elektronicznej w formacie edytowalnym oraz w co najmniej jednym egzemplarzu papierowym.
2. W dokumentacji muszą być zawarte opisy wszelkich cech, właściwości i funkcjonalności pozwalających na poprawną z punktu widzenia technicznego eksploatację rozwiązań.
3. W szczególności dokumentacja ta powinna zawierać:

Wymogi ogólne:

1. Pełna charakterystyka licencjonowania wszystkich elementów aplikacji środowiska.
2. Opis architektury technicznej:

- wyszczególnienie oraz opis powiązań wszystkich komponentów sprzętowych, systemowych i aplikacyjnych występujących lub wymaganych do poprawnej pracy aplikacji zgodnie z wymaganiami wydajności, funkcjonalności i bezpieczeństwa (minimalny, maksymalny, rekomendowany),

3. Konfiguracja musi obejmować wszystkie urządzenia wdrożone, zainstalowane w ramach budowy systemu IT.

4. Przykładowy zestaw wymaganych danych konfiguracyjnych obejmuje:
- serwery – parametry sprzętowe (procesor, pamięć, dyski, karty sieciowe, zasilanie, itp.),
- sieć (adresacja IP, itp.),
- podsystem dyskowy (punkty montowania/litery dysków, wolumeny logiczne, grupy wolumenowe, zasoby dyskowe, RAID, itp.),
- system operacyjny (parametry jądra, moduły, usługi, stos TCP/IP, itp.),
- klaster (węzły fizyczne, paczki klastrowe, kolejność przełączania, itp.),
- listę zainstalowanego oprogramowania, itp.,

2. Wymagania minimalne dla macierzy dyskowej:

L.p.	Element konfiguracji	Wymagania minimalne
1.	Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19”.
2.	Przestrzeń dyskowa	Macierz musi być wyposażona w minimum 14 dysków NVMe TLC lub MLC o pojemności nie mniejszej niż 7.68 TB. Nie dopuszcza się stosowania protokołu innego niż NVMe do obsługi dysków w macierzy. Macierz musi udostępniać co najmniej 75 TB pojemności użytecznej bez uwzględniania mechanizmów deduplikacji i kompresji zabezpieczonej RAID 6 z wraz z przestrzenią/dyskami SPARE. Macierz musi mieć możliwość obsługi co najmniej 670 TiB pojemności surowej (raw) na dyskach NVMe. Musi istnieć możliwość dalszego skalowania pojemności oraz wydajności macierzy (np. zmiana kontrolerów, rozbudowa o dodatkowe półki dyskowe). Nie dopuszcza się wirtualizacji zewnętrznych pamięci masowych. **Wymaganie nieobligatoryjne (parametr punktowany)** : macierz umożliwia rozbudowę do minimum 72 dysków SSD NVMe, dołączanych redundantnie za pomocą interfejsów min. 100Gb z wykorzystaniem RoCEv2. *Oferowana konfiguracja dyskowa musi oferować wydajność min. 230k IOPS przy bloku 16kB Random 80/20 R/W oraz włączonej redukcji danych (deduplikacja i kompresja).* *Powyższy wynik należy potwierdzić wydrukiem z oficjalnego konfiguratora producenta oferowanej macierzy oraz potwierdzony oświadczeniem przedstawiciela producenta oferowanej macierzy dyskowej (dostarczone najpóźniej wraz z dostawą macierzy).*
3.	Sposób zabezpieczenia danych	Macierz musi posiadać mechanizm RAID zabezpieczający przed utratą spójności danych w przypadku jednoczesnej awarii dwóch dowolnych dysków. Mechanizm realizowany sprzętowo za pomocą dedykowanego układu z wykorzystaniem puli wszystkich dysków twardych (tzw. wide-striping).

		Rozłożenie dysków w macierzy musi zapewniać redundancję pozwalającą na nieprzerwaną pracę i dostęp do wszystkich danych w sytuacji awarii pojedynczego komponentu sprzętowego typu: dysk, port, kontroler, zasilacz, kabel. Macierz musi umożliwiać definiowanie dysków „spare" lub odpowiadającej im przestrzeni dyskowej „spare". Wymagane zabezpieczenie minimum RAID-6.
4.	Kontrolery macierzowe	Macierz All-NVMe wyposażona w minimum 2 kontrolery macierzowe obsługujące protokoły blokowe i pracujące w trybie ALUA (Asymmetric Logical Unit Access). Oba kontrolery muszą jednocześnie aktywnie obsługiwać wolumeny. Oprogramowanie macierzy musi rozkładać obsługę wolumenów pomiędzy kontrolery i dążyć do ich równomiernego obciążenia. Każdy z kontrolerów musi być wyposażony w wielordzeniowe procesory x86 (każdy w minimum 16 fizycznych rdzeni). Z uwagi na kompatybilność z systemami operacyjnymi oraz aplikacjami występującymi w środowisku Zamawiającego, a listą rozkazów obsługiwanych przez procesory zainstalowane w oferowanym rozwiązaniu, Zamawiający zaakceptuje jedynie rozwiązania wyposażone w procesory firm Intel lub AMD. Zastosowany procesor musi wspierać standard PCIe Gen4. Każdy kontroler musi posiadać co najmniej 256GB pamięci RAM o szybkości 3200MT/s. Kontrolery muszą obsługiwać protokół FC, NVMeoF-FC na portach wystawionych do hostów (front-end).
5.	Interfejsy	Macierz musi być wyposażona, w co najmniej: • 4 karty 4 portowe (po 2 karty na kontroler) 64Gb FC z kompletem wkładek 32Gb SW. Musi istnieć możliwość wymiany wkładek na wkładki 64Gb FC SW • 2 porty (po 1 na kontroler) Ethernet min. 1Gb BaseT do zarządzania macierzą Wraz z macierzą musi zostać dostarczona infrastruktura sieci SAN z uwzględnieniem urządzeń przełączających dla sieci w architekturze 32gbps i zapewniających pracę redundantną dla podłączonych serwerów oraz innych urządzeń. Należy zapewnić 2 przełączniki SAN wyposażone w 8 aktywnych portów 32Gbps każdy przełącznik oraz 16 portów wolnych do dalszej rozbudowy. Każdy z przełączników musi wspierać następujące mechanizmy zwiększające poziom bezpieczeństwa: a) mechanizm tzw. Switch Binding, który umożliwia zdefiniowanie listy kontroli dostępu regulującej prawa urządzeń FC do podłączenia do przełącznika fabric

		b) mechanizm tzw. Port Binding, który umożliwia zdefiniowanie listy kontroli dostępu regulującej prawa hostów i urządzeń storage FC do podłączenia do portu przełącznika c) uwierzytelnianie (autentykacja) przełączników w sieci Fabric za pomocą protokołów FCAP d) uwierzytelnianie (autentykacja) urządzeń końcowych w sieci Fabric za pomocą protokołu DH-CHAP e) szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2. f) definiowanie wielu kont administratorów z możliwością ograniczenia ich uprawnień za pomocą mechanizmu tzw. RBAC (Role Based Access Control) g) definiowane kont administratorów w środowisku RADIUS, LDAP w MS Active Directory, Open LDAP, TACACS+ h) szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS i) obsługa SNMP v1 oraz v3 j) IP Filter dla portu administracyjnego przełącznika k) wgrywanie nowych wersji firmware przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP wykonywanie kopii bezpieczeństwa konfiguracji przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP l) Możliwość diagnozowania z poziomu przełącznika połączeń światłowodowych, Możliwość pomiaru połączenia (prędkość, opóźnienia, dystans), wbudowany generator przepływu danych, możliwość wykonywania poleceń FC ping, Pathinfo (FCtraceroute), możliwość podglądu ramek, monitorowanie stanu łącz, monitorowanie stanu urządzenia
6.	Sposób zarządzania	Zarządzanie macierzą dyskową musi być możliwe z poziomu interfejsu graficznego oraz linii poleceń. Oprogramowanie do zarządzania musi pozwalać na stałe monitorowanie stanu macierzy oraz umożliwiać konfigurowanie jej zasobów dyskowych. Narzędzie musi pozwalać na obserwację danych wydajnościowych oraz prezentację ich w postaci wykresów oraz czytelnych raportów. Wymagane jest monitorowanie bieżących parametrów pracy macierzy.
7.	Zarządzanie grupami dyskowymi oraz dyskami logicznymi	Macierz musi zapewniać możliwość dynamicznego zwiększania pojemności wolumenów logicznych oraz wielkości grup dyskowych (przez dodanie dysków) z poziomu kontrolera macierzowego bez przerywania dostępu do danych. 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.
8.	Thin Provisioning	Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów 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).
9.	Wewnętrzne kopie migawkowe	Macierz musi umożliwiać dokonywanie na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez konieczności wcześniejszego alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Wymagany jest mechanizm Redirect-on-wite (ROW) lub równoważny, który nie wymaga kopiowania oryginalnych danych przy ich zmianie po wykonaniu migawki. Macierz musi posiadać mechanizm uniemożliwiający jakiemukolwiek użytkownikowi (w tym administratorom) usunięcie migawkowej kopii danych przez zdefiniowany okres. Okres ten nie może zostać skrócony.
10.	Zdalna replikacja danych	Macierz musi umożliwiać zdalną replikację danych typu online do innej macierzy z tej samej rodziny z wykorzystaniem protokołu FC i IP. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. Musi istnieć możliwość jednoczesnej natywnej replikacji w trybach: synchronicznym i asynchronicznym za pośrednictwem różnych infrastruktur (FC i IP). Oprogramowanie musi zapewniać funkcjonalność zawieszania i ponownej przyrostowej resynchronizacji kopii z oryginałem oraz zamiany ról oryginału i kopii (dla określonej pary wolumenów logicznych) z poziomu interfejsu administratora.
11.	Ciągła dostępność do danych	Macierz musi umożliwiać replikowanie danych synchronicznie z drugą taką macierzą i zapewniać – w przypadku awarii i całkowitej niedostępności jednej z macierzy – ciągłą pracę systemów działających na platformie przetwarzania danych i korzystających z zasobów pamięci masowych. Opisane powyżej przełączenie między macierzami musi odbywać się w sposób automatyczny i transparentny dla korzystających z dysków logicznych macierzy serwerów i aplikacji. Opisana funkcjonalność musi zapewniać integrację z co najmniej Microsoft Cluster Service

		oraz platformą wirtualizacyjną VMware (VMware vSphere Metro Storage Cluster). Rozwiązanie musi umożliwiać hostom jednoczesny zapis do obu macierzy dla tego samego wolumenu.
12.	Zarządzanie wydajnością	Macierz musi umożliwiać konfigurację gwarancji wydajności typu QoS w postaci ustawień kilku poziomów priorytetów obsługi.
13.	Kompresja i deduplikacja danych	Macierz musi zapewniać kompresję i deduplikację danych na poziomie blokowym. Musi istnieć możliwość uruchomienia deduplikacji na poziomie pojedynczych wolumenów logicznych. Kompresja i deduplikacja nie mogą być realizowane za pomocą zewnętrznego urządzenia lub oprogramowania.
14.	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 dla protokołu FC: Windows Server 2022, Red Hat 9.x, VMware 8.x, SLES 15. Macierz musi wspierać podłączenie następujących systemów operacyjnych dla protokołu NVMeoF-FC: Red Hat 9.x, VMware 8.x.
15.	Wysoka dostępność	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 dwóch niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy. Macierz musi umożliwiać wykonywanie aktualizacji mikrokodu macierzy w trybie online bez wyłączania żadnego z interfejsów macierzy. Macierz musi umożliwiać zdalne zarządzanie macierzą oraz automatyczne informowanie centrum serwisowego o awarii. Producent macierzy musi gwarantować 100% dostępność do danych dla pojedynczej macierzy. Wymagane potwierdzenie na publicznej stronie producenta na żądanie Zamawiającego.
16.	Dodatkowe wymagania	Oferowana macierz dyskowa musi być fabrycznie nowa, wyprodukowana **nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z oficjalnego kanału dystrybucyjnego producenta na rynek polski.** Zamawiający zastrzega sobie, aby Wykonawca na żądanie Zamawiającego przedłożył oświadczenie Producenta

		oferowanego sprzętu, w języku polskim, potwierdzające pochodzenie sprzętu z autoryzowanego kanału sprzedaży z Polski.
17.	Gwarancja	Minimum 5-letnia gwarancja producenta w miejscu instalacji. Gwarantowany czas naprawy w minimum 6h, możliwość zgłoszenia awarii przez siedem dni w tygodniu, 24 godziny na dobę. Czas reakcji serwisu maksymalnie następny dzień roboczy. Zamawiający ma możliwość pozostawienia wszystkich typów nośników danych zawartych w urządzeniu. W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z macierzą oraz oprogramowania wewnętrznego macierzy. Gwarancja na sprzęt musi być dostarczona i realizowana przez organizację serwisową producenta sprzętu.

3. Przełączniki agregacyjne (dalej również rdzeniowe) LAN – zestaw przełączników do pracy redundantnej (2 sztuki)

	Minimalne wymaganie dotyczące <u>jednej sztuki</u> przełącznika
1.	Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack. System operacyjny (firmware) dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej.
2.	Wymagane parametry fizyczne: a) możliwość montażu w stelażu/szafie 19” b) wysokość maksymalna 1U c) głębokość urządzenia nie większa niż 46 cm d) waga urządzenia nie większa niż 15kg e) dwa wewnętrzne redundantne zasilacze 230V AC typu hot-swap (nie dopuszcza się rozwiązania zewnętrznego). Każde urządzenie musi zostać dostarczone z 2 zasilaczami z możliwością wymiany w trakcie pracy urządzenia (ang. hot-swap). f) zakres temperatur pracy ciągłej co najmniej od 0 do +45 °C g) zakres wilgotności pracy co najmniej 5% - 95% h) maksymalny pobór mocy nie większy niż: 430W i) minimum 1 port USB lub mini/micro-usb
3.	Urządzenie musi być wyposażone w minimum 4 wentylatory z możliwością wymiany pojedynczego wentylatora w trakcie pracy urządzenia (ang. hot-swap).
4.	Przełącznik musi zostać dostarczony z następującymi interfejsami mogącymi działać równocześnie: ● 48 portów 25GE SFP28 z obsługą modułów 25G-SR, 10G-SR, 10G-LR, 10G-ER, 1G-LX, 1G-SX ● 8 portów 100G QSFP28 z obsługą modułów 40G-SR, 40G-LR, 100G-SR, 100G-LR Wszystkie porty 25G SFP28 oraz 100G QSFP28 muszą być dostępne od frontu urządzenia.
5.	Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności: a) Zarządzanie stosem poprzez jeden adres IP

	b) Do min. 9 jednostek w stosie c) Magistrala stackująca o wydajności minimum 400Gb/s d) Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation) e) Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree f) Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia. Zamawiający dopuszcza, aby możliwość łączenia w stosy była realizowana za pomocą portów typu uplink. W ramach postępowania należy dostarczyć od producenta oryginalny kabel do stackowania (DAC) 100G QSFP28 o długości 1m.
6.	Układ przełączający o wydajności min. 4Tbps, wydajność przełączania przynajmniej 2000 Mpps
7.	Obsługa min. 286 000 adresów MAC
8.	Wbudowana pamięć RAM min. 8 GB Bufor pakietów minimum: 32 MB Procesor wielordzeniowy. Minimalne taktowanie procesora 2200MHz
9.	Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 4 GB
10.	Obsługa min. 4090 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)
11.	Możliwość skonfigurowania min. 1000 interfejsów vlan interface SVI działających równocześnie.
12.	Obsługa ramek jumbo o wielkości min. 9216 bajtów
13.	Obsługa protokołu BFD oraz LACP
14.	Obsługa protokołu VRRP dla IPv4 i IPv6
15.	Wsparcie dla protokołów 802.1d (STP), 802.1s (MSTP), 802.1w (RSTP), 802.1ag, 802.3ah, 802.3ad.
16.	Obsługa protokołów routingu OSPF, OSPFv3, IS-IS, IS-ISv6, BGPv4, BGPv4+, RIP, RIPng. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania
17.	Obsługa min. 322 000 tras dla routingu IPv4
18.	Obsługa min. 161 000 tras dla routingu IPv6
19.	Obsługa funkcjonalności VRF (Virtual Routing and Forwarding). Wymagana minimalna ilość VRF: 4000
20.	Obsługa protokołów związanych z obsługą ruchu typu multicast: a) IGMP v1, v2 i v3 b) IGMP Snooping v2 i v3 c) PIM-SM, PIM-SSM, PIM-DM d) MSDP i MLD e) minimum 120 000 tras multicast dla IPv4 i minimum 60 000 tras multicast dla IPv6 f) Multicast VPN
21.	Minimalny rozmiar tablicy ARP – minimum 272 000 wpisów
22.	Obsługa sFlow

23.	Przełącznik musi posiadać funkcjonalność DHCP Serwer, DHCP Snooping, DHCP Relay, DHCP Klient
24.	Mechanizmy związane z zapewnieniem bezpieczeństwa sieci: a) min. 3 poziomy dostępu administracyjnego poprzez konsolę b) obsługa sprzętowo reguł ACL. Możliwość utworzenia minimum 18000 reguł ACL a) zarządzanie urządzeniem z wykorzystaniem SNMPv3, SSHv2 c) możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP d) obsługa mechanizmów związanych z ochroną protokołu STP: BPDU Protection lub równoważne, Root Protection lub równoważne e) możliwość synchronizacji czasu zgodnie z NTP lub SNTP
25.	Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach: • klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP • wsparcie dla mechanizmów QoS z wykorzystaniem algorytmu karuzelowego, np.: WRR, WDRR, DRR, WFQ, WRED
26.	Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA).
27.	Wymagane opcje zarządzania: a) możliwość lokalnej obserwacji ruchu na określonym porcie b) plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC) c) wsparcie dla skryptów Python d) wsparcie dla RMON i RMON2 e) dedykowany port konsoli, zgodny ze standardem RS-232 f) dedykowany port zarządzający out-of-band Ethernet Base-T
28.	Wraz z urządzeniami muszą zostać dostarczone: a) pełna dokumentacja w języku polskim lub angielskim b) dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana
29.	Wsparcie dla funkcjonalności VXLAN L2 i L3. Minimum 2000 tuneli VxLAN. Jeżeli obsługa powyżej funkcjonalności wymaga dodatkowej licencji to w ramach niniejszego postępowania Zamawiający wymaga jej dostarczenia.
30.	Wsparcie dla technologii MPLS, w tym L3 VPN. Jeżeli funkcjonalność MPLS wymaga licencji to należy ją dostarczyć w ramach niniejszego postępowania
31.	Wsparcie dla funkcjonalności M-LAG lub MC-LAG
32.	Wsparcie dla funkcjonalności DCBx, PFC, ECN, RDMA, RoCE, OpenFlow (minimum 1.3), NETCONF, Ansible
33.	Wsparcie dla funkcjonalności telemetry: gRPC i ERSPAN
34.	Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy
35.	Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich.
36.	Zamawiający wymaga**, aby przełączniki posiadały 5-letni serwis gwarancyjny** świadczony przez Wykonawcę (lub autoryzowany serwis) na bazie wsparcia serwisowego wykupionego u

	producenta oferowanych urządzeń. Naprawa urządzenia w trybie 9x5xNBD-S. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia. Zamawiający na etapie dostawy będzie wymagał oświadczenia producenta potwierdzającego nabycie oraz zarejestrowanie serwisu gwarancyjnego na Zamawiającego. Wszystkie koszty związane z naprawami gwarancyjnymi nie mogą obciążać Zamawiającego (np. koszty wysyłki). W celu zapewnienia odpowiedniego poziomu świadczonych usług Wykonawca lub autoryzowany serwis producenta musi posiadać status autoryzowanego partnera serwisowego przyznawany przez producenta dla oferowanych urządzeń, a usługa serwisu musi być świadczona w języku polskim.
37.	Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres serwisu gwarancyjnego dla urządzeń.

4. Prace wdrożeniowe i konfiguracyjne dotyczące zestawu 2 przełączników rdzeniowych

Zamawiający wymaga dostarczenia oraz montażu i konfiguracji przełączników rdzeniowych sieci. Wraz z przełącznikami należy dostarczyć wszystkie niezbędne do całego wdrożenia moduły SFP+ /SFP28 oraz przewody połączeniowe umożliwiające podłączenie wszystkich urządzeń do istniejącej struktury sieci.

Wykonawca przygotuje projekt wdrożenia przełączników, a po akceptacji projektu przez Zamawiającego przeprowadzi wdrożenie, który będzie obejmować minimum:

1. Aktualizację firmware przełączników do najnowszej stabilnej wersji
2. Konfigurację portów do zarzadzania (management port)
3. Konfigurację sieci wirtualnych przełącznika na podstawie obecnej infrastruktury
4. Konfigurację i readresację całej struktury sieci
5. Konfigurację agregacji połączeń do serwerów pomiędzy przełącznikami
6. Konfigurację agregacji połączeń dla przełączników dostępowych
7. Konfigurację syslog dla przełączników
8. Konfigurację protokołu SNMP zgodnie z obecnym systemem monitoringu
9. Konfigurację użytkowników administracyjnych przełącznika zgodnie z wytycznymi bezpieczeństwa
10. Uruchomienie dostępu poprzez SSH oraz interface www z HTTPs. Certyfikaty HTTPs należy wygenerować oraz zainstalować na urządzeniach.
11. Uruchomienie autoryzacji użytkowników do konsoli w oparciu o lokalnych użytkowników. Nie może być możliwy dostęp do konsoli bez wcześniejszej autoryzacji. Konsola powinna wylogować użytkownika w przypadku nieaktywności. Hasła lokalnych kont muszą być szyfrowane, niedopuszczalne jest przechowywanie haseł czystym tekstem.
12. Konfigurację autoryzacji użytkowników SSH oraz WWW w oparciu o serwer radius. Wykonawca zainstaluje i skonfiguruje serwery RADIUS (podstawowy oraz zapasowy), wobec których będzie następowała autoryzacja użytkowników przechowywanych w katalogu LDAP.
13. Konfigurację serwera czasu NTP – przełączniki musza mieć skonfigurowaną synchronizację czasu w oparciu o serwery NTP 0.pl.pool.ntp.org, 0.pl.pool.ntp.org. Ustawienie właściwej strefy czasowej.
14. Wykonawca przekaże konfiguracje przełączników do dokumentacji oraz skonfiguruje automatyczną kopię urządzeń sieciowych.
15. Wszystkie porty na urządzeniach sieciowych zostaną opisane poprzez wykonawcę w sposób określony przez Zamawiającego.

16. Wykonawca wyłączy protokoły CDP oraz LLDP na portach dostępowych (np. dla stacji roboczych i telefonów) Natomiast na połączeniach pomiędzy przełącznikami należy zostawić włączone protokoły.
17. Wykonawca skonfiguruje protokół MSTP w ramach dostarczonych przełączników.
18. Wykonawca przeprowadzi konfigurację VLANów na przełącznikach wskazanych na etapie wdrożenia przez Zamawiającego (wraz z dedykowanym vlanem do zarządzania przełącznikami sieciowymi)
19. Wykonawca na urządzeniach zdefiniuje wskazany na etapie wdrożenia serwer DNS oraz domenę wyszukiwania na urządzeniach sieciowych.
20. W ramach wdrożenia Wykonawca przedstawi możliwe do uruchomienia dodatkowe zabezpieczenia dla dostarczanych urządzeń. Zamawiający na etapie wdrożenia zdecyduje, które zabezpieczenia należy uruchomić.
21. Jeżeli dostarczane urządzenia będą dysponować API umożliwiającym konfigurację urządzeń należy przygotować skrypty odpowiadające konfiguracji (python, ansible) w celu zarządzania zmianą konfiguracji.

Zamawiający może wymagać skonfigurowania dodatkowych funkcji przełączników, jeśli podczas wdrożenia zajdzie taka potrzeba.

5. Instruktaże

Zamawiający wymaga przeprowadzenia instruktaży dla swoich administratorów zgodnie z poniższym opisem:

a) Instruktaż podstawowy (wdrożeniowy) – odbędzie się przy okazji wdrożenia i konfiguracji przełączników w siedzibie Zamawiającego, jego przedstawiciele będą uczestniczyć w wykonywanych pracach.

b) Instruktaż z zakresu funkcji, konfiguracji wdrożonych przełączników sieci LAN (powdrożeniowy), dla grupy 2 średniozaawansowanych administratorów, minimum 1 maksimum 2 dniowy, obejmujący cały zakres wdrożenia. Instruktaż będzie podzielony na sloty około 4 godzinne. Harmonogram instruktaży zostanie przygotowany przez Wykonawcę i przedstawiony Zamawiającemu do akceptacji.

c) Instruktaż powdrożeniowy musi zawierać elementy warsztatowe i opierać się na zadaniach praktycznych realizowanych w przygotowanym laboratorium (LAB) z oferowanymi lub podobnymi przełącznikami. LAB musi być przygotowany w najbardziej zbliżonej wersji oprogramowania zastosowanej podczas wdrożenia na przełącznikach Zamawiającego.

d) Instruktaże muszą być prowadzone przez praktyka posiadającego co najmniej 5-letnie doświadczenie w zakresie wdrażania, konfiguracji przełączników sieci LAN, systemów firewall oraz posiadającego ważny certyfikat inżynierski potwierdzający kompetencje w zakresie zabezpieczania i konfiguracji sieci LAN/WAN.

6. Dokumentacja powykonawcza

Wykonawca dostarczy co najmniej w formie elektronicznej dokumentację powykonawczą. Dokumentacja powinna zawierać wszystkie dane dostępowe do konfigurowanych urządzeń, systemów, schematy podłączenia urządzeń do sieci LAN, opis konfiguracji dostarczonych i wdrożonych przełączników, opis wdrożonych rozwiązań.

7. System wirtualizacji oraz serwerowe środowisko operacyjne

Zaoferowane licencje muszą uprawniać do uruchamiania w klastrze wirtualnym nielimitowanej ilości maszyn wirtualnych, oferowanego Serwerowego Systemu Operacyjnego - SSO. Dostarczone licencje muszą obejmować wszystkie rdzenie wszystkich procesorów zainstalowanych w serwerach S1 i S2

(łącznie 32 rdzenie dla obydwu serwerów) Serwerowy System Operacyjny musi posiadać następujące, wbudowane cechy minimalne:

1. możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym,
2. możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny,
3. możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych,
4. możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (Hypervizor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci,
5. wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy,
6. wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy,
7. automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading),
8. wbudowane wsparcie instalacji i pracy na wolumenach, które:

– pozwalają na zmianę rozmiaru w czasie pracy systemu,
– umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
– umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
– umożliwiają zdefiniowanie list kontroli dostępu (ACL),

9. wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość,
10. wbudowane szyfrowanie dysków
11. możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET,
12. możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów,
13. wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych,
14. graficzny interfejs użytkownika,
15. zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
16. wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play),
17. możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu,
18. dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa,
19. możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:

– podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
– usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach,

pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:

a) podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
b) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
c) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,

– zdalna dystrybucja oprogramowania na stacje robocze,
– praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,
– centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:

a) dystrybucję certyfikatów poprzez http,
b) konsolidację CA dla wielu lasów domeny,
c) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,

– szyfrowanie plików i folderów,
– szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
– możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,
– serwis udostępniania stron WWW,
– wsparcie dla protokołu IP w wersji 6 (IPv6),
– możliwość szyfrowania maszyn wirtualnych
– możliwość uruchomienia nieograniczonej liczby kontenerów Hyper-V
– możliwość tworzenia repliki maszyn wirtualnych bez ograniczenia wielkości dla pojedynczego magazynu
– możliwość uruchomienia magazynów danych zdefiniowanych programowo
– wbudowane mechanizmy wirtualizacji (Hypervizor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:

a) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
b) obsługi ramek typu jumbo frames dla maszyn wirtualnych,
c) obsługi 4-KB sektorów dysków,
d) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,
e) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model),
f) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet,
g) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath),
h) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego,
i) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty,
j) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF

8. Usługa aktualizacji oraz konfiguracji oraz migracji środowiska bazodanowego.
Wymagane jest dostarczenie nowej licencji serwera baz danych wraz z pakietem wsparcia na okres 5 lat

Wymagane jest przeniesienie środowiska istniejącej bazy danych ORACLE do systemu operacyjnego Microsoft Windows Server Standard w wersji 2025 lub równoważny system operacyjny spełniający wymagania z pkt 10 wraz z aktywnym wsparciem producenta. W ramach aktualizacji bazy danych niezbędne jest zastosowanie nowej licencji silnika bazy danych ORACLE DB SE w najwyższej dostępnej wersji lub równoważnej spełniające kryteria wskazane w punkcie 8 oraz umożliwiające pełne przeniesienie i wykorzystanie istniejących instancji baz danych środowisk Infomedica firmy ASSECO POLAND

Wszystkie prace musza być przeprowadzone przez certyfikowanego inżyniera Oracle, który posiada aktywny certyfikat min. Oracle Certified Associate (OCA). Zakres prac do wykonania został przedstawiony w poniższych punktach:

1. Analiza wymagań migracji serwera bazy danych w tym inwentaryzacja istniejącego środowiska
2. Po analiza przekazanie propozycji migracji
2.1 Migracja przy pomocy exportu/importu danych z wykorzystaniem narzędzi DataPump, czas migracji zależny od wielkości baz danych i wydajności podsystemu dyskowego/sieciowego
2.2 Migracja z minimalizacją przestoju pracy środowiska produkcyjnego z wykorzystaniem kopii bezpieczeństwa RMAN (aktualne środowisko klienta musi pracować w trybie Archivelog)
3. Instalacja możliwe najnowszego systemu operacyjnego Oracle Linux, kompatybilnego z wersją docelową oprogramowania baz danych, jeżeli jest wymagana aktualizacja wersji bazy danych z 11g do 19c i minimalizacja przestoju to wtedy podjęte będą następujące kroki:
3.1 Instalacja Oracle Linux 7.9 będącego ostatnią wersją systemu wspierającą bazę 11g
3.2 Migracja z wykorzystaniem RMAN wersji 11g
3.3 Aktualizacja bazy z 11g do 19c
3.4 Aktualizacja systemu operacyjnego Oracle Linux do wersji 8.10 z 7.9
4. Uruchomienie produkcyjne systemu
5. Analiza po-migracyjna i optymalizacja baz danych na podstawie wykonania raportu "dobrych praktyk" Oracle

Wszystkie opisane pracę muszą zostać podsumowane w dokumentacji przed i po wdrożeniowej wraz z potwierdzeniem wykonania testów działania bazy w środowisku IT i wszystkich aplikacji z niej korzystających (AMMS,InfoMedica)

W ramach usługi Wykonawca dostarczy i zainstaluje dedykowany serwer bazy danych wyposażony w 1 procesor 16 rdzeniowy o wydajności min. 135 pkt w teście SPEC CPU 2017 Integer Rate na podstawie wyników publikowanych na witrynie spec.org dla oferowanego modelu serwera. Pamięć operacyjna 256GB RAM, zainstalowane 2 dyski w standardzie SSD o pojemności min. 480GB każdy dysk, praca w układzie RAID 1, zainstalowane 2 interfejsy 10/25gbps z modułami optycznymi SR 25gbps oraz 2 interfejsy FC32GBPS oraz 1 interfejs LAN RJ45 do zarządzania serwerem, dwa zasilacze redundantne oraz środowisko zarządzania z możliwością przejęcia pełnej konsoli graficznej dla administratora w połączeniu zdalnym do serwera. Zainstalowane środowisko Windows hiper-v z wykorzystaniem licencji posiadanej przez Zamawiającego (MS Windows 2022 Standard). Zostanie przez Wykonawcę przygotowana maszyna wirtualna z środowiskiem Oracle Linux na której wykonawca skonfiguruje, uruchomi, zmigruje i zaktualizuje, istniejące środowisko bazodanowe.

9. Wymagania funkcjonalne dla silnika bazy danych

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, 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:
4. Oprogramowanie bazy danych ze względu na zgodność z systemem operacyjnym oraz platformą sprzętową,
5. Systemy operacyjne używane do uruchamiania serwerów bazy danych ze względu na zgodność z platformą sprzętową.
6. Dostępność narzędzi migracji baz danych pomiędzy platformami na poziomie fizycznym (kopiowanie / konwersja plików danych) oraz logicznym (narzędzia eksportu / importu).
7. 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)
8. Wsparcie protokołu XA.
9. Wsparcie standardu JDBC 3.0.
10. Zgodność ze standardem ANSI/ISO SQL 2003 lub nowszym.
11. Wbudowana obsługa wyrażeń regularnych zgodna ze standardem POSIX dostępna z poziomu języka SQL jak i procedur/funkcji składowanych w bazie danych.
12. RDBMS musi zapewniać niezależność platformy systemowej dla oprogramowania klienckiego od platformy systemowej bazy danych.
13. RDBMS musi zapewniać przetwarzanie transakcyjne wg. reguł ACID z zachowaniem spójności i maksymalnego 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.
14. RDBMS musi posiadać możliwość zagnieżdżania transakcji – możliwość uruchomienia niezależnej transakcji wewnątrz transakcji nadrzędnej.
15. 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.
16. Dostępność poziomu serializowanego poziomu izolowania transakcji (Serializable).
17. Możliwość zmiany domyślnego trybu izolowania transakcji (Read Commited) na inny (Read Only, Serializable) za pomocą komend serwera bazy danych.
18. 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 Code Page 1250 oraz PC 852. Automatyczna konwersja znaków pomiędzy różnymi ustawieniami stron kodowych po stronie klienta i serwera bazy danych.
19. Możliwość migracji bazy danych utrzymujących dane znakowe w 8-bitowej stronie kodowej do Unicode.
20. Możliwość definiowania w przestrzeni danych (plików) dla danych użytkownika obszarów o innym niż domyślny rozmiarze bloku.
21. Możliwość bez dodatkowych ograniczeń przechowywania wierszy, których rozmiar przekracza rozmiar bloku bazy danych.
22. 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.
23. 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 tabele, na której oparty jest widok zmaterializowany.
24. Możliwość szybkiego odświeżania danych w widoku zmaterializowanym na podstawie mechanizmu identyfikacji zmian w danych źródłowych.
25. Brak formalnych ograniczeń na liczbę tabel i indeksów w bazie danych oraz na ich rozmiar (liczbę wierszy).
26. Kosztowy model optymalizacji instrukcji SQL.

27. 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).
28. Możliwość uwzględnienia korelacji wartości występujących w niezależnych kolumnach tabeli w modelu statystyk optymalizatora kosztowego.
29. 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.
30. 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.
31. 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. kursorów pobierających paczki danych (wiele wierszy za jednym pobraniem) oraz wspierać mechanizmy transakcyjne (np. zatwierdzanie bądź wycofanie transakcji wewnątrz procedury).
32. Możliwość kompilacji procedur składowanych w bazie do postaci kodu binarnego (biblioteki dzielonej).
33. Możliwość deklarowania wyzwalaczy (triggerów) na poziomie instrukcji DML (INSERT, UPDATE, DELETE) wykonywanej natabeli, 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).
34. W przypadku, gdy w wyzwalaczu na poziomie instrukcji DML wystąpi błąd zgłoszony przez motor bazy danych bądź 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.
35. Możliwość wykonania równoczesnych operacji DML (Insert/Update/Delete) na tej samej tabeli.
36. Powinna istnieć możliwość autoryzowania użytkowników bazy danych za pomocą rejestru użytkowników założonego w bazie danych bądź mechanizmu zewnętrznego w stosunku do bazy danych.
37. Przywileje użytkowników bazy danych powinny być określane za pomocą przywilejów systemowych (np. prawo do podłączenia 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.
38. 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).
39. 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.
40. Możliwość uruchomienia bazy danych w środowisku klastra wielu aktywnych serwerów bazy danych. Ilość socketów CPU w klastrze nie przekracza 2.

41. Zwiększenie bądź zmniejszenie liczby serwerów obsługujących klastrową bazę danych nie może powodować konieczności reorganizacji fizycznej bazy danych (struktura plików danych)
42. Zwiększenie bądź zmniejszenie liczby serwerów obsługujących klastrową bazę danych nie może powodować konieczności reorganizacji logicznej struktury baz danych (tabel / indeksów).
43. Unieruchomienie jednego z serwerów klastra bazy danych nie może powodować braku dostępu do jakiejkolwiek części danych – baza danych musi być nadal dostępna za pośrednictwem funkcjonujących dalej serwerów.
44. Możliwość kontynuacji prący użytkowników podłączonych do serwera klastrowej bazy danych, który uległ awarii. Wymagana jest możliwość przeniesienia sesji na inny serwer oraz automatycznego powiadomienia aplikacji o wykonaniu przełączenia.
45. Każdy z serwerów klastra musi mieć możliwość uspójnienia lub odtworzenia całej bazy danych w sytuacji awarii nośników lub nagłego zatrzymania innego serwera, który utrzymywał w buforze bazy danych zmodyfikowane, ale niezapisane bloki danych.
46. Obraz bazy danych (metadane, obiekty bazy danych, stan danych) w klastrowej bazie danych musi być niezależny od serwera, do którego zostało nawiązane połączenie.
47. Licencja typu ASFU z wsparciem podstawowym producenta bazy na okres 5 lat
48. Przeznaczenie-usługi wdrażanego oprogramowanie i EDM.

10. Kryteria równoważności dla systemu operacyjnego dla środowiska baz danych

Licencja Serwerowego Systemu Operacyjnego (SSO), uprawniającej do uruchomienia min. 2 maszyn wirtualnych na serwerze posiadającym łącznie 16 rdzeni procesorów. Parametry minimalne dla SSO:

1. Współpraca z procesorami o architekturze x86-64 bit
2. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.
3. Pojedyncza licencja musi obsłużyć serwer fizyczny wyposażony w 1 procesor 16 rdzeniowy.
4. Pojedyncza licencja musi umożliwiać na instalację min 2 wystąpień wirtualnych (min 2 maszyny wirtualne)
5. Praca w roli klienta domeny Microsoft Active Directory.
6. System musi być wspierany przez producenta oprogramowania do 2030 r. (wsparcie techniczne, aktualizacje bezpieczeństwa)
7. Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie funkcjonalności Microsoft Windows Server 2022.
8. Możliwość uruchomienia roli klienta i serwera czasu (NTP).
9. Możliwość uruchomienia roli serwera plików w z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
10. Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
11. Możliwość uruchomienia roli serwera stron WWW.
12. W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.
13. W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego.
14. Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania.
15. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
16. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
17. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
    a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
    b. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
18. Wbudowany mechanizm klasyfikowania i indeksowania pliko w (dokumentów) w oparciu o ich zawartość
19. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET.
20. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.

21. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
22. Zlokalizowane w języku polskim lub angielskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
23. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
24. Mechanizmy logowania w oparciu o:
    a. login i hasło,
    b. karty z certyfikatami (smartcard),
    c. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
25. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla:
    a. określonych grup użytkowników.
    b. zastosowanej klasyfikacji danych,
    c. centralnych polityk dostępu w sieci,
    d. centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
26. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
27. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
28. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
29. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
30. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
31. Możliwość implementacji usług sieciowych: DHCP oraz DNS wspierający DNSSEC.
32. Możliwość implementacji usług katalogowej oparte o LDAP i pozwalającej na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
    a. ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
    b. odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
    c. zdalna dystrybucja oprogramowania na stacje robocze,
33. Możliwość implementacji Centrum Certyfikatów (CA) z obsługą klucza publicznego i prywatnego) umożliwiające:

a. Dystrybucję certyfikatów poprzez http,
b. Konsolidację CA dla wielu lasów domeny
c. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
d. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
e. szyfrowanie plików i folderów,
f. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
g. szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi,
h. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail - over) oraz rozłożenia obciążenia serwerów,
i. serwis udostępniania stron WWW,
j. wsparcie dla protokołu IP w wersji 6 (IPv6),
k. wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,

l. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie nieograniczonej liczby aktywnych środowisk wirtualnych systemów operacyjnych (liczba ograniczona parametrami fizycznymi serwera),
m. możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (Hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
n. mechanizmy wirtualizacji mające wsparcie dla:
    a. dynamicznego podłączania zasobów dyskowych typu hot plug do maszyn wirtualnych,
    b. obsługi ramek typu jumbo frames dla maszyn wirtualnych.
    c. możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.
    d. możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
    e. wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
    f. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
    g. mechanizm konfiguracji połączenia VPN do platformy Azure.
    h. wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.
    i. mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.
    j. możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server Standard)

11. Dedykowany serwer dla bazy danych:

L.p.	Element konfiguracji	Wymagania minimalne
1	Obudowa	Maksymalnie 2U RACK 19 cali (wraz z szynami montażowymi i prowadnicą kabli, umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia). Serwer wyposażony w: - zdejmowanym panel przedni z zamkiem, chroniącym przed nieuprawionym dostępem do dysków -czujnik otwarcia obudowy współpracującego z BIOS/UEFI.
2	Płyta główna	Płyta główna umożliwiająca instalację do dwóch procesorów fizycznych, wspierająca zastosowanie procesorów od 8 do 40 rdzeni, mocy do min. 270W i taktowaniu CPU do min. 3.4GHz.
3	Procesor	Min. jeden procesor max. 12-rdzeniowy, x86 - 64 bity, pracujący z częstotliwością bazową min. 2.8GHz i osiągający w teście SPECrate2017_int_base wynik nie gorszy niż 132 punkty dla testowanej konfiguracji z dwoma procesorami. Wynik testu dla oferowanego modelu serwera musi być zamieszczony na oficjalnej stronie internetowej (www.spec.org).
4	Pamięć operacyjna	Min. 256 GB RDIMM DDR4 w modułach pamięci o pojemności min. 32GB RDIMM 3200MT/s każdy. Płyta główna z minimum 32 slotami na pamięć i umożliwiająca instalację do minimum 8 TB pamięci RAM (przy zastosowaniu odpowiednich procesorów).

		Obsługa zabezpieczeń: Advanced ECC, Online Spare, Memory Mirroring, Memory Patrol Scrubbing Serwer umożliwiający instalowanie pamięci Intel Optane DC Persistent Memory przy zainstalowaniu odpowiednich procesorów.
5	Złącza rozszerzeń	Serwer musi mieć możliwość wykorzystania do 6 złącz PCI-Express min. generacji 4, w tym min. 2 sloty x8 (szybkość slotu – bus width) i min. 4 sloty x16 (szybkość slotu – bus width) dla konfiguracji z dwoma procesorami. Wszystkie sloty muszą umożliwiać na instalację kart pełnej wysokości (full height).
6	Dysk twardy	Zatoki dyskowe gotowe do zainstalowania min. 8 dysków SFF typu hot-plug SAS/SATA/SSD, 2,5". Opcja rozbudowy/rekonfiguracji serwera o dodatkowe 16 dysków typu hot-plug, SAS/SATA/SSD, 2,5" montowanych z przodu obudowy. Zainstalowane min. 2 dyski 480GB SAS typu hot-plug
7	Kontroler	Serwer wyposażony w kontroler sprzętowy z min. 4GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, min. 16 portowy (16 dedykowanych linii SAS do podłączenia dysków SAS), obsługujący poziomy: RAID 0/1/10/5/50/6/60. Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie.
8	Interfejsy sieciowe LAN	Zainstalowana karta sieciowa z min. 4 portami Ethernet 1Gb RJ-45. Karta nie może zajmować slotów PCI-ex. Zainstalowana karta sieciowa z dwoma portami 10Gb SFP+ wraz z modułami SFP+. Zainstalowana karta Fibre Channel min. 2 portowa 32Gbit.
9	Karta graficzna	Zintegrowana karta graficzna umożliwiająca wyświetlenie obrazu min. 1920 x 1200@60Hz
10	Porty	Min. 5 portów USB 3.0 (w tym 1 port z przodu obudowy i 2 wewnętrzne) Min. 1 port VGA
11	Napęd	Możliwość rozbudowy serwera o wewnętrzny napęd DVD-RW Możliwość rozbudowy serwera o port szeregowy
12	Chłodzenie i zasilanie	Zestaw wentylatorów redundantnych typu hot-plug Redundantne zasilacze typu hot-plug o mocy max. 850W każdy.
13	Diagnostyka i bezpieczeństwo.	Serwer wyposażony w moduł TPM 2.0 Możliwość zainstalowania elektronicznego panelu diagnostycznego dostępnego z przodu serwera pozwalającego uzyskać informacje o stanie: procesora, pamięci, wentylatorów, zasilaczy, temperaturze.
	Karta/moduł zarządzający	Niezależna od system operacyjnego, posiadająca funkcjonalność: • Monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski (fizyczne i logiczne). • Wsparcie dla pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP.

14		• Dostęp do karty zarządzającej poprzez dedykowany port RJ45 z tyłu serwera • Dostęp do karty możliwy - z poziomu przeglądarki webowej (GUI) - z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP) - poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface). • Wbudowane narzędzia diagnostyczne. • Obsługa mechanizmu automatycznego połączenia karty z serwisem producenta sprzętu, automatycznego przesyłania alertów, zgłoszeń serwisowych i zdalnego monitorowania. • Wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników • Przesyłanie alertów poprzez e-mail. • Obsługa zdalnego serwera logowania (remote syslog). • Wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD. • Mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie. • Funkcja zdalnej konsoli szeregowej przez SSH (wirtualny port szeregowy). • Monitorowanie zasilania oraz zużycia energii przez serwer w czasie z możliwością graficznej prezentacji. • Konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping). • Zdalna aktualizacja oprogramowania (firmware). • Zarządzanie grupami serwerów, w tym: - tworzenie i konfiguracja grup serwerów - sterowanie zasilaniem (wł/wył) - ograniczenie poboru mocy dla grupy (power caping) - aktualizacja oprogramowania (firmware) - wspólne wirtualne media dla grupy. • Możliwość równoczesnej obsługi przez min. 5 administratorów. • Autentykacja dwuskładnikowa (Kerberos). • Wsparcie dla Microsoft Active Directory • Obsługa TLS i SSH. • Możliwość trwałego zablokowania dokonania obniżenia wersji oprogramowania układowego (firmware) serwera. • Wsparcie dla algorytmów CNSA • Wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API • Możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)

15	Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Min. Microsoft Windows Server 2019, 2022 Min. Red Hat Enterprise Linux (RHEL): 8.6, 9.0 Min. SUSE Linux Enterprise Server (SLES) 15 Min. VMware ESXi 7.0 U3, 8.0
16	Wsparcie techniczne	Dostarczony sprzęt i oprogramowanie zarządzające objęte trzyletnim wsparciem technicznym z możliwością zgłaszania problemów w trybie 5x8, czas reakcji do 4 godzin od zgłoszenia, gwarantowany czas rozpoczęcia naprawy w następnym dniu roboczym w miejscu instalacji. Obsługa zgłoszeń serwisowych/gwarancyjnych dotyczących sprzętu i oprogramowania w języku polskim. Usługa wsparcia technicznego musi być świadczona przez autoryzowany serwis producenta oferowanych urządzeń. Możliwość rozszerzenia usługi gwarancyjnej do 5 lat realizowanej przez serwis producenta serwera z gwarantowanym czasem naprawy 6 godzin i pozostawieniem uszkodzonych dysków u zamawiającego.
17	Inne	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Deklaracja zgodności CE.

12. Zasilacz awaryjny:

L.p.	**Element konfiguracji**	**Wymagania minimalne**
1	Moc znamionowa	10 kVA / 10 kW
2	Wejście	złącze zasilania x1, złącze zasilania trybu obejścia (bypass) x1
3	Wyjście	Współczynnik mocy:1 Napięcie: 380/400/415 V AC Częstotliwość: 50/60 ± 0.05 Hz THDu ≤ 2% (obciążenie liniowe) Przeciążalność (< 33°C) 106-125%: 5 minut 126-150%: 1 minuta. > 150%: 500 milisekund
4	Sprawność	AC-AC Do 96,5% Tryb ECO 99%
5	Prąd ładowania	Do 8 A
6	Poziom hałasu	maksymalnie 55 dB
7	Czas podtrzymania	Minimum 7 min. dla obciążenia 50% (min. 5 kW)
8	Wyświetlacz	Graficzny wyświetlacz LCD z obsługą wielu języków
9	Interfejsy komunikacyjne	Złącze MINI x1 (możliwość instalacji kart SNMP, Modbus, Relay), styki bezpotencjałowe x4, port USB x1, port RS-232x1, port RS-485 x1, port REPO/ROO x1
10	Zgodność	CE, UL/cUL, RCM, TISI, EAC, BIS, KC, BSMI

13. Zakres usług gwarancyjnych dla dostarczonego oprogramowania aplikacyjnego oraz środowiska sprzętowego.

Minimalny okres gwarancji dla dostarczonych urządzeń oraz subskrypcji i wsparcia technicznego dla oprogramowania wchodzącego w skład rozwiązania wynosi min. 3 lata

Wady

1. W okresie gwarancji Wykonawca będzie zobowiązany do nieodpłatnego usuwania Wad Przedmiotu Zamówienia rozumianych jako Awaria lub Błąd lub Usterka zgodnie z definicjami jak poniżej:
    - **Awaria -** Kategoria Wady w Oprogramowaniu lub Infrastrukturze Sprzętowej powodująca brak działania lub niepoprawne działanie Przedmiotu Zamówienia u Zamawiającego, uniemożliwiające jego użytkowanie. Sytuacja, w której dane rozwiązanie w ogóle nie funkcjonuje lub nie jest możliwe realizowanie istotnych funkcjonalności Komponentów/Produktów Przedmiotu Zamówienia
    - **Błąd** – kategoria Wady Oprogramowania oznaczającą jego funkcjonowanie niezgodne z opisem w Dokumentacji oraz SOPZ, powodujące błędne zapisy w bazie danych lub uniemożliwiające działanie mniej istotnej funkcjonalności w Systemie
    - **Usterka -** Należy przez to rozumieć kategorię Wady w Oprogramowaniu lub Infrastrukturze Sprzętowej oznaczającą funkcjonowanie niezgodne z opisem Dokumentacji oraz SOPZ, nie wpływającą istotnie na funkcjonowanie dostarczanego rozwiązania u Zamawiającego, utrudniającą pracę Użytkownikom Zamawiającego w stopniu minimalnym.
2. Przyjęcie zgłoszenia Wady przez Wykonawcę, odbywać się będzie poprzez dostępny on-line System Zgłaszania i przyjmowania uwag oraz Wad (dalej zwany SZ) przy czym:
    A. System Zgłoszeń dostarczy Wykonawca (będzie on utrzymywany i administrowany przez Wykonawcę), wpis zgłoszenia do SZ będzie dokonywał Zamawiający,
    B. za skuteczne przyjęcie zgłoszenia Wady uważa się będzie wprowadzenie przez Zamawiającego wpisu do SZ zawierającego opis zgłaszanej Wady i termin jej zgłoszenia; w razie trudności z dostępem on-line do SZ, zgłoszenia Wady mogą odbywać się także telefonicznie pod dedykowanym numerem telefonu lub pisemnie na formularzu przesyłanym na ustalony adres e-mail, opcjonalnie faksem, których numery i adresy zostaną podane przez Wykonawcę w terminie 15 dni roboczych od dnia podpisania Umowy wraz ze wzorem formularza zgłoszenia Wady. Dedykowana linia telefoniczna dla zgłoszeń Zamawiającego będzie wymagała podania kodu PIN w celu połączenia z przyjmującym zgłoszenie po stronie Wykonawcy.
3. W przypadku, w którym wykonanie Umowy związane będzie z modernizacją lub rozbudową istniejącego oprogramowania, gwarancja obejmuje całość oprogramowania modernizowanego lub rozbudowywanego.
4. Gwarancja musi zapewniać wymianę uszkodzonego sprzętu, kabli i elementów oraz zapewniać dostęp do aktualizacji oprogramowania, bez wiedzy i wsparcia technicznego producenta.

5. W ramach gwarancji Wykonawca będzie świadczył następujące usługi:
   A. Usuwanie Wad w dostarczonym Przedmiocie Zamówienia w przypadku stwierdzenia przez Zamawiającego Wady w jego działaniu, w terminach określonych poniżej:

Tabela 1. Usługi gwarancji dla Infrastruktury sprzętowej:

KWALIFIKACJA ZGŁOSZENIA WADY	OKRES DOSTĘPNOŚCI WYKONAWCY	ROZWIĄZANIE ZASTĘPCZE*	CZAS REAKCJI WYKONAWCY	CZAS NAPRAWY
AWARIA	24/7/365	niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 14 dni od czasu przyjęcia zgłoszenia
USTERKA		nie dotyczy	niezwłocznie nie później niż 5 dni roboczych od dnia przyjęcia zgłoszenia	niezwłocznie nie później niż 30 dni od dnia przyjęcia zgłoszenia

***** nie dotyczy sprzętu zastępczego

Tabela 2. Usługi gwarancji dla oprogramowania

KWALIFIKACJA ZGŁOSZENIA WADY	OKRES DOSTĘPNOŚCI WYKONAWCY	ROZWIĄZANIE ZASTĘPCZE	CZAS REAKCJI WYKONAWCY	CZAS NAPRAWY
AWARIA	W dni robocze pomiędzy 8.00 a 16.00. Zgłoszenie przesłane po 16.00, traktowane jest jak zgłoszenie przyjęte w następnym dniu roboczym o 8.00	niezwłocznie, nie później niż 24 godzin od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 24 godzin od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 72 godziny od czasu przyjęcia zgłoszenia
BŁĄD		nie dotyczy	niezwłocznie nie później niż 7 dni robocze od dnia	niezwłocznie nie później niż 30 dni roboczych od dnia

			przyjęcia zgłoszenia	przyjęcia zgłoszenia
USTERKA		nie dotyczy	niezwłocznie nie później niż 7 dni roboczych od dnia przyjęcia zgłoszenia	niezwłocznie nie później niż 30 dni roboczych od dnia przyjęcia zgłoszenia

B. dopuszcza się zmianę kwalifikacji zgłoszenia Wady, po uprzedniej zgodzie Zamawiającego. Do czasu potwierdzenia zmiany kwalifikacji, uznaje się za obowiązującą kwalifikację pierwotną,
C. czasy naprawy mogą być inne niż wskazane w powyższych tabelach, jeżeli Zamawiający zaakceptuje zmianę kwalifikacji zgłoszenia, o której mowa w punkcie B,
D. w przypadku braku możliwości usunięcia Wady lub przedstawienia rozwiązania zastępczego zdalnie, Wykonawca zobowiązany jest do świadczenia gwarancji bezpośrednio w lokalizacji Zamawiającego,
E. usunięcie Wady Oprogramowania, nastąpi poprzez przekazanie poprawki lub nowej wersji. Każda nowa poprawka lub nowa wersja musi posiadać unikalny numer lub oznaczenie,

14. Pozostałe ustalenia:

1. System Zgłoszeń, który zostanie udostępniony przez Wykonawcę, ma dodatkowo pozwalać na prowadzenie rejestru wykonanych czynności gwarancyjnych, ewidencję wszystkich zgłoszeń gwarancyjnych, opis zmian w konfiguracji Oprogramowania; prowadzenie rejestru zgłoszeń jest obowiązkiem Wykonawcy.
2. Gwarancja na urządzenia musi być świadczona przez firmę autoryzowaną przez producenta lub jego przedstawicielstwo w przypadku, gdy Oferent nie posiada takiej autoryzacji.
3. Zamawiający ustala procedurę zdalnego dostępu Wykonawcy do Oprogramowania: Wykonawca drogą elektroniczną poprzez e-mail, prześle Zamawiającemu wniosek o uzyskanie zdalnego dostępu do Oprogramowania, wskazując co najmniej:
   a. imię i nazwisko pracownika Wykonawcy, któremu zostanie przyznany dostęp,
   b. nazwa i adres IP zasobu (bazy danych/oprogramowania), który zostanie udostępniony,
   c. usługi sieciowe, które zostaną udostępnione,
   d. okres czasu, na który będzie aktywowany dostęp,
   e. numer zgłoszenia gwarancyjnego,
   f. przyczyna złożenia wniosku,
   g. przyczyna złożenia wniosku,
   h. opis czynności, które zostaną wykonane,

4. Procedura odpowiedzi Zamawiającego na złożony wniosek:
    a. osoba wyznaczona przez Zamawiającego zaopiniuje wniosek i w formie elektronicznej poprzez e-mail odpowie, podając informację o zgodzie lub jej braku.
    b. po zakończeniu prac Wykonawca ma obowiązek przesłać Zamawiającemu raport z wykonanych prac z wykorzystaniem zdalnego dostępu, podając czas ich trwania i zakres.
    c. każdy zdalny dostęp do Oprogramowania musi być przez Wykonawcę odnotowany w Systemie Zgłoszeń,
    d. dostęp do zasobów Zamawiającego musi być zgodny z obowiązującą u niego polityką bezpieczeństwa.
5. Wykonawca zobowiązuje się do przekazania Zamawiającemu informacji o nowych wersjach oprogramowania drogą elektroniczną na wskazany adres e-mail Zamawiającego,
6. Wykonawca zobowiązuje się do świadczenia usług w postaci konsultacji, porad, dodatkowej konfiguracji, tworzenia nowych raportów, wsparcia technicznego w zakresie wdrożenia oraz użytkowania oprogramowania, przy czym:
    - usługi będą świadczone w dni robocze w godzinach od 8.00 do 16.00 w języku polskim, w siedzibie Zamawiającego lub za uzgodnieniem Stron, jako prace świadczone zdalnie
    - tryb zgłaszania: telefonicznie, e-mail, faxem lub poprzez Elektroniczny System Zgłoszeń, konsultacje i porady będą udzielane na bieżąco podczas rozmowy telefonicznej lub w postaci elektronicznej, jednak nie później niż w ciągu 3 dni roboczych od skierowania zapytania. Jeżeli nie jest możliwe wykonanie usługi w ciągu 3 dni roboczych, Wykonawca uzgodni z Zamawiającym inny termin konsultacji lub porady, jeżeli Zamawiający wyrazi na to zgodę.

Uwaga:

W przypadku zapisu terminu jako:

- Dzień Roboczy należy rozumieć każdy dzień od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy.
- Godziny Robocze należy rozumieć godziny od 8.00 do 16.00 w każdym Dniu Roboczym.

W innych przypadkach należy rozumieć jako dzień kalendarzowy.