**Załącznik nr 8** – Opis przedmiotu zamówienia

Nr sprawy: **ZR-078/D/RZ/2024**

Zamówienie pn. „*Zakup i instalacja macierzy i serwerów*”

ZAMAWIAJACY: **Miejskie Wodociągi i Kanalizacja w Bydgoszczy - spółka z o.o.**

Opis przedmiotu zamówienia

pn.: „*Zakup i instalacja macierzy i serwerów*”

W związku z rozbudową i modernizacją istniejącej infrastruktury serwerowej,   
Zamawiający składa zamówienia na :

1. Dostawę:
2. macierzy – 2 szt.
3. serwerów – 2 szt.
4. centralnej stacji zarządzającej – 1 szt.
5. przełączników sieciowych – 4 szt.
6. szafy rackowej – 1 szt.
7. Usługi wdrożeniowe:
8. Instalację i konfigurację sprzętu.
9. Instalację i konfigurację VMWare na nowych serwerach.
10. Wsparcie techniczne.

Dostarczony sprzęt musi być fabrycznie nowy, musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski. Wymagane oświadczenie producenta, że oferowany do przetargu sprzęt spełnia ten wymóg. Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz muszą być objęte gwarancją producenta, potwierdzoną przez oryginalne karty gwarancyjne. Oferent zobowiązany jest dostarczyć wraz z ofertą, szczegółową specyfikację techniczną oferowanego sprzętu.

1. **MACIERZ – 2 sztuki**
2. **Wymagania:**
   1. Macierz musi mieć możliwość zainstalowania w standardowej szafie 19”
   2. Macierz musi cechować brak pojedynczego punktu awarii.
   3. Macierz musi posiadać dwa redundantne kontrolery pracujące w trybie active-active wymienialne bez przerywania pracy. Kontrolery macierzy muszą obsługiwać interfejsy NVMe do napędów dyskowych. Kontrolery muszą wykorzystywać powszechnie dostępną technologię procesorową Intel lub AMD.
   4. Całkowita wysokość oferowanej macierz w szafie rack nie może przekraczać 2U.
   5. Pamięć podręczna macierzy musi być nie mniejsza niż 256 GB (po 128 GB na każdy z kontrolerów) z możliwością rozbudowy do 512 GB
   6. Wymagane jest niemniej niż 8 portów 32 Gb/s Fibre Channel dla dostępu do macierzy od strony hostów. Macierz powinna posiadać dodatkowo co najmniej 4 porty 10/25 GbE z obsługą iSCSI do komunikacji z hostami poprzez protokół iSCSI obsadzone wkładkami światłowodowymi 10 Gb SFP+`. Wymagana jest obsługa adapterów z portami 10 GbE, FC/FC-NVMe 32 Gb/s i 64 Gb/s
   7. Macierz musi wspierać następujące protokoły komunikacji z serwerami: Fibre Channel/FC-NVMe, iSCSI, iSER, NVMe over TCP
   8. Macierz powinien wpierać zasilanie z dwóch niezależnych źródeł prądu.
   9. Macierz musi obsługiwać napędy 2,5” i 3,5” we właściwych obudowach. Macierz musi obsługiwać dyski SAS 1,2 TB, 1,8 TB oraz 2,4 TB 10000 obr/min, dyski 6TB, 8 TB, 10TB, 12 TB, 14TB, 16TB, 18TB, 20 TB 7200 rpm oraz 1,92TB, 3,84TB, 7,68TB, 15,36TB oraz 30,72TB SSD. Macierz musi zapewniać możliwość używania różnych dysków tego samego typu – odpowiednio 2,5” i 3,5” – w ramach jednej obudowy. Wszystkie obsługiwane dyski muszą wykorzystywać interfejs połączeniowy SAS co najmniej 12 Gb/s oraz każdy powinien posiadać dwa porty SAS. Wymagana obsługa standardu hot-swap.
   10. Macierz musi obsługiwać napędy Storage Class Memory z interfejsem NVMe.
   11. Macierz musi umożliwiać jednoczesną instalację i używanie wszystkich wspieranych napędów z interfejsem NVMe w ramach obudowy kontrolera.
   12. Macierz musi obsługiwać połączenia do półek dyskowych oraz do dysków w standardzie SAS 12 Gb/s
   13. Macierz musi obsługiwać co najmniej 400 dysków, z możliwością rozbudowy do co najmniej 800 w systemie złożonym z dwóch lub więcej macierzy.
   14. Macierz musi posiadać pojemność co najmniej 100 TiB efektywnej przestrzeni widzianej przez serwery bez zastosowania redukcji danych po uwzględnieniu przestrzeni zapasowej oraz poziomu RAID odpornego na awarię dwóch dysków przy zastosowaniu nośników Flash o pojemności pojedynczego nośnika nie większej niż 20 TB.
   15. Macierz musi obsługiwać poziomy RAID obsługujące logiczne lustro oraz konfigurację z wyliczaniem parzystości, odporną na awarię 1 i 2 dysków, zapewniające dystrybucję pomiędzy wszystkimi dyskami w grupie RAID zarówno informacji o parzystości jak również przestrzeni zapasowej. Grupy RAID z parzystością muszą być możliwe do utworzenia z dowolnej ilości dysków pomiędzy 6 a 128 z dokładnością do jednej sztuki.
   16. Oferowany poziom zabezpieczeń RAID musi umożliwiać rozbudowę online grupy RAID o kolejne napędy w zakresie od jednego co najmniej 40 napędów jednocześnie.
   17. Macierz musi wykorzystywać połączenia punkt-punkt do dysków twardych.
   18. Macierz musi umożliwiać jednoczesne stosowanie półek dyskowych obsługujących dyski 2,5” oraz 3,5” w odpowiednich obudowach. Półki dyskowe 2,5” muszą umożliwiać instalację co najmniej 24 napędów dyskowych 2,5”. Półki dyskowe 3,5” muszą umożliwiać instalację co najmniej 12 napędów dyskowych 3,5”. Macierz musi umożliwiać podłączenie półek dyskowych wysokiej gęstości tzn. obsługujące co najmniej 80 dysków i gęstości upakowania co najmniej 18 dysków na każde U wysokości obudowy w szafie rack.
3. **Wymagania co do funkcjonalności:**
   1. Macierz musi mieć możliwość wirtualizacji zasobów znajdujących się na innych macierzach dyskowych, w szczególności pochodzących od HPE, IBM, Fujitsu, Dell EMC i HDS. Zasoby zwirtualizowane muszą korzystać z wszystkich funkcjonalności macierzy które dotyczą również dysków wewnętrznych. Jeżeli funkcjonalność wymaga licencji, nie jest ona obecnie wymagana, ale musi być dostępna w ofercie producenta na dzień składania ofert i możliwa do dokupienia w przyszłości.
   2. Macierz musi posiadać funkcjonalność zarządzania całością dostępnych zasobów dyskowych, zarówno wewnętrznych jak i zewnętrznych (zwirtualizowanych) z jednej konsoli administracyjnej. Zarządzanie musi być dostępne poprzez interfejs GUI (WWW) oraz interfejs linii poleceń (Command Line Interface). Dostęp do linii poleceń poprzez połączenie szyfrowane.
   3. Musi istnieć możliwość bezpośredniego monitoringu stanu w jakim w danym momencie macierz się znajduje. Dane o parametrach wydajnościowych macierzy muszą być dostępne w postaci wykresów w interfejsie GUI. Prezentowane muszą być dane o wydajności kontrolerów, wolumenów i interfejsów za okres co najmniej 60 dni.
   4. Musi istnieć funkcjonalność Cache dla procesu odczytu.
   5. Musi istnieć funkcjonalność Mirrored Cache dla procesu zapisu.
   6. Musi istnieć możliwość wyłączenia cache dla poszczególnych wolumenów
   7. Macierz musi posiadać system podtrzymania zawartości pamięci cache na wypadek awarii zasilania realizowany poprzez zapis danych z pamięci cache kontrolerów do pamięci typu flash lub równoważny zapewniający co najmniej taki sam czas przechowywania danych.
   8. Macierz musi optymalizować wykorzystanie napędów różnego rodzaju poprzez automatyczną identyfikację obciążenia fragmentów wolumenów w zarządzanych zasobach dyskowych (wewnętrznych jak i zewnętrznych, zwirtualizowanych) oraz ich automatyczną migracje na napędy o odpowiedniej wydajności. Macierz musi posiadać możliwość wykorzystania mechanizmu optymalizacji umiejscowienia danych pomiędzy przynajmniej trzema rodzajami dysków spośród wszystkich dostępnych rodzajów obsługiwanych napędów, jak również przy wykorzystaniu dwóch dowolnych z tychże. Opisany powyżej proces optymalizacji musi posiadać funkcję włączenia/wyłączenia na poziomie pojedynczego wolumenu. Jeżeli funkcjonalność wymaga licencji, należy takową zaoferować na całą macierz bez ograniczeń ilościowych czy pojemnościowych.
   9. Macierz musi umożliwiać automatyczne równoważenie obciążenia w ramach grupy/puli dysków tego samego typu. Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla całej macierzy w maksymalnej konfiguracji.
   10. Macierz musi zapewniać odporność na chwilowy zanik napięcia zasilającego.
   11. Minimalna ilość wspieranych wirtualnych dysków logicznych (LUN) dla całej (globalnej) puli dyskowej zbudowanej w oparciu o jedną macierz musi wynosić co najmniej 8000.
   12. Macierz musi obsługiwać funkcjonalności mapowania wolumenów do hostów lub grup hostów, tak aby inne hosty/grupy hostów nie miały do nich dostępu.
   13. Macierz musi zapewniać funkcjonalność udostępniania przestrzeni bez konieczności fizycznego alokowania wolnego miejsca na dyskach (thin provisioning). Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla całej macierzy w maksymalnej konfiguracji.
   14. Macierz musi mieć możliwość wykonania kopii danych typu Point-In-Time (PiT) wolumenów. Zasoby źródłowe oraz docelowe kopii PiT mogą być zabezpieczone różnymi poziomami RAID i być umiejscowione na różnych technologicznie dyskach stałych obsługiwanych przez system, w szczególności na zasobach wirtualizowanych macierzy. Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla całej macierzy w maksymalnej konfiguracji.
   15. Kopie danych typu PIT muszą być tworzone w trybach kopii pełnej (klon) oraz kopii wskaźników (migawka), incremental (kopiowanie tylko bloków zmienionych pomiędzy kolejnymi wykonaniami kopii), multitarget (wiele kopii z jednego źródła), cascaded (kopia z kopii). Kopie danych typu PIT muszą być również możliwe do utworzenia w formie niezmienialnej (immutable).
   16. Macierz musi obsługiwać minimum 255 kopi migawkowych per wolumen, minimum 15000 łącznie w całym systemie.
   17. Macierz musi umożliwiać tworzenie niezmienialnych (immutable) kopii lokalnych wolumenów dla potrzeb szybkiego odzyskiwania danych w przypadku np. celowego uszkodzenia danych. Kopie muszą być tworzone w wydzielonej przestrzeni na macierzy. Macierz musi posiadać funkcjonalność definiowania polityk wykonywania i przechowywania kopii które powinny obejmować minimum częstotliwość i czas wykonywania kopii oraz ich retencję. Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla całej macierzy w maksymalnej konfiguracji.
   18. Macierz musi obsługiwać grupy spójności wolumenów do celów kopiowania i replikacji.
   19. Macierz musi mieć możliwość wykonywania replikacji synchronicznej i asynchronicznej wolumenów logicznych pomiędzy różnymi typami macierzy dyskowych. Zasoby źródłowe kopii zdalnej oraz docelowe kopii zdalnej mogą być zabezpieczone różnymi poziomami RAID i egzystować na dowolnych obsługiwanych przez macierz napędach. Replikacja musi być realizowana zarówno przy użyciu interfejsów Fibre Channel jak i protokołu IP. Macierz musi umożliwiać replikację również z innymi modelami macierzy w ramach tej samej rodziny macierz. Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla całej macierzy w maksymalnej konfiguracji.
   20. Macierz musi mieć możliwość wykonania migracji wolumenów logicznych pomiędzy różnymi typami zasobów dyskowych wewnątrz macierzy, bez zatrzymywania aplikacji korzystającej z tych wolumenów. Wymaga się aby zasoby źródłowe podlegające migracji oraz zasoby do których są migrowane mogły być zabezpieczone różnymi poziomami RAID i zlokalizowanymi na różnych technologicznie napędach obsługiwanych przez system w tym zasobach wirtualizowanych. Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla maksymalnej konfiguracji.
   21. Macierz musi posiadać funkcjonalność zwiększania rozmiaru wolumenów.
   22. Macierz musi posiadać funkcjonalność zarządzania ilością operacji wejścia-wyjścia wykonywanych na danym zasobie macierzy. Zarządzanie musi być możliwe poprzez określenie maksymalnej ilości operacji I/O na sekundę lub przepustowości określonej w MB/s dla danego zasobu lub poprzez oba te parametry jednocześnie. Wymagana jest możliwość określania ww. parametrów dla zasobów macierzy takich jak wolumen, grupa wolumenów, host, klaster hostów. Jeżeli funkcjonalność ta wymaga licencji należy ją dostarczyć dla maksymalnej konfiguracji macierzy.
   23. Macierz musi posiadać funkcjonalność kompresji danych online, gdzie dane zapisywane w macierzy są kompresowane w locie i zapisywane na dyskach w postaci skompresowanej, a przy odczycie dane są również w locie dekompresowane i w takiej postaci przesyłane poza macierz. Skompresowane dane muszą być możliwe do składowania na wszystkich wspieranych rodzajach dysków. Operacja kompresji nie może wymagać alokacji innej przestrzeni dyskowej niż ta, która jest niezbędna do zapisania skompresowanych danych. Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla całej macierzy w oferowanej konfiguracji.
   24. Macierz musi posiadać funkcjonalność deduplikacji danych online, gdzie dane zapisywane w macierzy są deduplikowane w locie i zapisywane na dyskach w postaci po usunięciu duplikatów. Operacja deduplikacji nie może wymagać alokacji innej przestrzeni dyskowej niż ta, która jest niezbędna do zapisania zdeduplikowanych danych. Producent macierz musi udostępniać oprogramowanie pozwalające na estymację stopnia deduplikacji wolumenów. Zdeduplikowane dane muszą być możliwe do składowania na wszystkich wspieranych rodzajach dysków. Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla całej macierzy w oferowanej konfiguracji.
   25. Funkcjonalność reducji danych (kompresja i deduplikacja) musi być możliwa do zdefiniowania, włączenia/wyłączenia z dokładnością do jednego wolumenu.
   26. Macierz musi posiadać funkcjonalność migracji danych z innych macierzy dyskowych bez przerywania dostępu danych dla serwerów (import danych) z wykorzystaniem interfejsów FC oraz iSCSI. Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla nieograniczonej ilości migrowanych macierzy.
   27. Macierz musi umożliwiać stworzenie konfiguracji odpornej na awarię pojedynczej półki dyskowej.
   28. Macierz musi posiadać możliwość stworzenia konfiguracji aktywnego klastra, która przy wykorzystaniu dwóch urządzeń w dwóch lokalizacjach zapewni konfigurację wysokiej dostępności (HA-high availability) tzn. dostęp serwerów do tego samego zestawu LUNów prezentowanych z macierzy w każdej z lokalizacji. W sytuacji awarii jednej z dwóch macierzy wolumeny prezentowane do serwerów muszą dostępne w sposób ciągły bez żadnej przerwy. Klaster musi umożliwiać przyjmowanie zapisu i odczytu do obu macierzy w klastrze - host musi komunikować się zawsze z najbliższą macierzą wskazywaną poprzez mechanizm preferowanej ścieżki minimalizując w ten sposób ruch na ISL przełączników SAN. Replikacja danych między macierzami w klastrze wysokiej dostępności musi odbywać się po sieci SAN. Klaster musi umożliwiać zarówno automatyczną naprawa klastra po awarii jak i automatyczny powrót kierunku replikacji do stanu sprzed awarii. Klaster musi mieć możliwość powiększania wolumenów klastrowych bez rozłączania lub zatrzymywania replikacji w parze. Rozwiązanie musi być niezależne od platformy serwerowej i systemu operacyjnego. Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla całej macierzy w maksymalnej konfiguracji.
   29. Macierz musi posiadać funkcjonalność szyfrowania składowanych danych zarówno z użyciem dysków samoszyfrujących jak i bez konieczności używania dedykowanych dysków. Zarządzanie kluczami szyfrującymi musi być możliwe zarówno w trybie lokalnym jak i zdalnym poprzez zastosowanie serwera zarządzającego kluczami. Licencja na tę funkcjonalność jest wymagana dla całej macierzy, bez ograniczeń ilościowych czy pojemnościowych.
   30. Macierz musi umożliwiać stworzenie konfiguracji wysokiej dostępności z innymi modelami macierzy z tej samej rodziny urządzeń. Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla całej macierzy w maksymalnej konfiguracji.
   31. Macierz musi posiadać możliwość liniowej skalowalności parametrów wydajnościowych zasobów dyskowych oraz ilości obsługiwanych dysków (do co najmniej 800) poprzez dodanie do systemu kolejnej macierzy tego samego typu (łącznie co najmniej 2), przy zachowaniu jednolitego i wspólnego zarządzania zasobami dyskowymi.
   32. Wraz z oferowaną macierzą dyskową należy zaoferować oprogramowanie współpracujące z macierzą, które umożliwia:
       1. Monitorowanie zasobów macierzy w zakresie pojemności i wydajności
       2. Zbieranie danych o wydajności, pojemności i konfiguracji za okres przynajmniej 1 roku.
       3. Eksport danych wydajnościowych do pliku
       4. Tworzenie raportów o monitorowanych urządzeniach, ich wydajności i pojemności i użyciu zasobów storage.
       5. Tworzenie konfigurowalnych, wielowarunkowych alertów i polityk.
       6. Wykrywanie w trybie inline zagrożenia ransomware i generowanie alertów z tym związanych.
       7. Optymalizację umiejscowienia danych pod kątem wydajności (tiering)
       8. Planowanie pojemności i wydajności na podstawie analizy danych historycznych.
       9. Analizę przepływów danych dla potrzeb wykrywania i usuwania problemów (troubleshooting)
       10. Monitorowanie macierzy innych producentów w tym przynjamniej NetApp, Dell EMC, IBM, PureStorage, Hitachi
       11. Monitorowanie hostów połączonych z macierzą, w szczególności pracujących pod kontrolą VMWare.
       12. Monitorowanie przełączników Fibre Channel (Brocade i Cisco)
   33. Oprogramowanie musi zapewniać uprawnienia do usługi chmurowej o analogicznym zakresie działania. Oprogramowanie musi zostać dostarczone ze wsparciem na okres równy lub dłuższy od okresu wsparcia oferowanej macierzy.
   34. Sterowniki do obsługi wielościeżkowego dostępu do wolumenów, awarii ścieżki i rozłożenia obciążenia po ścieżkach dostępu muszą być dostępne dla podłączanych systemów operacyjnych. Jeżeli zastosowanie tych sterowników wymaga licencji, musi być dostarczona dla podłączanych systemów operacyjnych i/lub podłączanych serwerów zależnie od sposobu licencjonowania. Macierz może również wykorzystywać sterowniki systemu operacyjnego.
4. **Inne** 
   1. Macierz musi być fabrycznie nowa (data produkcji nie późniejsza niż 6 miesięcy przed dostawą), musi pochodzić z autoryzowanego kanału dystrybucji producenta na terenie Polski i być objęta serwisem producenta na terenie Polski.
   2. Producent macierzy nie może pochodzić z kraju, na który zostały nałożone sankcje przez członka NATO, ani mieć nałożone takie sankcje bezpośrednio.
   3. Macierz musi być objęta serwisem gwarancyjnym producenta przez okres 60 miesięcy ze zgłaszaniem problemów w trybie 24 godziny przez 7 dni w tygodniu oraz z gwarantowanym czasem naprawy do 24 godzin. W ramach serwisu muszą być dostępne nowe wersje oprogramowania dla macierzy oraz poprawki.

**II. SERWER – 2 sztuki** (wymagania minimalne)

1. **Obudowa**
   1. Obudowa Rack o wysokości maksymalnie 1U z możliwością instalacji minimum 10 dysków 2.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.
   2. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne lub/i dedykowany przenośny panel operatora - serwer musi posiadać możliwość monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) nie dopuszcza się bezpośredniej komunikacji bezprzewodowej z procesorem serwisowym dopuszcza się wyłącznie połączenie bezpośrednie np. USB czy dedykowanego złącza diagnostycznego, procesory serwisowe z komunikacją bezprzewodową muszą mieć możliwość całkowitej dezaktywacji komunikacji radiowej.
2. **Płyta główna**
   1. Płyta główna z możliwością zainstalowania minimum dwóch procesorów.
   2. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
3. **Chipset** - Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
4. **Procesor**
   1. Zainstalowane dwa procesory mające minimum 16 rdzeni, minimum 2.0GHz, klasy x86 osiągające w teście Spec.org Int Rate 2017 wynik baseline minimum 275 pkt w konfiguracji dwuprocesorowej.
   2. Wynik dla oferowanego serwera musi być dostępny na stronie https://spec.org w momencie składania oferty.
5. **RAM**
   1. Minimum 0,5TB DDR5 RDIMM w kościach minimum 32GB 4800MT/s, na płycie głównej powinny znajdować się minimum 32 sloty przeznaczone do instalacji pamięci.
   2. Wymagane jest w pełni optymalne obsadzenie pamięci RAM (wypełnienie równomierne wszystkich kanałów pamięci).
   3. System musi mieć możliwość rozbudowy do 8 TB DDR5 3DS RDIMM
   4. **Zabezpieczenia pamięci RAM:**
6. SDDC
7. ADDDC
8. Bounded Fault detection / correction
9. Memory mirroring
10. ECC detection/correction
11. **Gniazda PCI**
    1. Minimum trzy sloty x16 GEN5.
    2. Poza gniazdami PCIe dodatkowy slot OCP 3.0 PCIe5.0 x16.
12. **Interfejsy sieciowe/FC/SAS**
    1. Minimum cztery interfejsy sieciowe 10/25Gb SFP28 + kable DAC, w redundantnych kartach sieciowych.
    2. Minimum dwa interfejsy 16Gb FC
13. **Dyski twarde** - Zainstalowane minimum dwa dyski M.2 SSD Read Intensive o pojemności minimum 480GB
14. **Kontroler RAID -** Opcjonalny kontroler RAID – nawet 8GB cache / flash i obsługujący do 10 dysków. Zainstalowany w dedykowanym slocie dla kontrolerów dyskowych - niezajmujący miejsca w slocie PCIe.
15. **Wbudowane porty**
    1. Minimum 1x USB 3.2, 1x USB 2.0, opcjonalny port VGA dostępny z przodu serwera. Dedykowany port do zarządzania i diagnostyki dostępny z przodu serwera.
    2. Minimum 2x USB 3.2, 1x USB 2.0, VGA port, RJ45 dla procesora serwisowego dostępny z tyłu serwera
    3. Minimum 1x USB 3.2 dostępny wewnątrz serwera
16. **Video -** Zintegrowana karta graficzna z wbudowaną dedykowaną pamięcią minimum 16MB, umożliwiająca wyświetlenie rozdzielczości minimum 1920x1200 przy częstotliwości odświeżania minimum 60Hz.
17. **GPU** - Niewymagane
18. **Wentylatory** - Redundantne, Hot-Swap, posiadające redundantne silniki w każdym wentylatorze. Z uwagi na wysokie TDP procesorów muszą osiągać prędkość minimum 27k obrotów na minutę. Gwarancja poprawnego działania serwera nawet w temp. 35° C.
19. **Zasilacze** - Redundantne, Hot-Swap minimum 1100W każdy. Posiadające certyfikat 80Plus Titanium.
20. **Bezpieczeństwo**
    1. Opcjonalny panel zamykany na klucz służący do ochrony nieautoryzowanego dostępu do dysków twardych.
    2. Opcjonalny czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
    3. Moduł TPM 2.0
    4. Power-ON-Password oraz hasło administracyjne dla BIOS/UEFI
    5. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane zdalnie poprzez dostarczone oprogramowanie zarządzające.
21. **Diagnostyka** - Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy lub dołączany poprzez dedykowany port, umożliwiający wyświetlenie informacji o stanie serwera.
22. **Karta Zarządzania** - Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:
    1. zdalny dostęp do graficznego interfejsu Web karty zarządzającej
    2. zdalny dostęp poprzez SSH do CLI procesora serwisowego
    3. obsługę IPMI 2.0, SNMP v3/v1, CIM-XML, DCMI 1.5, Redfish DMTF
    4. przekierowanie portu szeregowego przez IPMI oraz SSH
    5. zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, temperatury: Otoczenia, CPU, pamięci DIMM)
    6. Out-of-Band (OOB) monitorowanie obciążenia CPU/Pamięci/IO oraz całego systemu
    7. szyfrowane połączenie (TLS min TLS 1.2) oraz autentykacje i autoryzację użytkownika
    8. możliwość zamontowania zdalnych wirtualnych napędów, (obrazy ISO) minimum 4 obrazy iso jednocześnie w czasie jednej sesji
    9. możliwość montowania obrazów ISO z lokalnej stacji zarządzającej poprzez przeglądarkę oraz poprzez współdzielone zasoby sieciowe minimum NFS/CIFS/HTTPS
    10. wirtualną konsolę z dostępem do myszy, klawiatury
    11. wirtualną konsolę oraz montowanie obrazów ISO bez instalacji dodatkowych komponentów Java czy AciveX (musi działać w oparciu o HTML5)
    12. wsparcie dla IPv6
    13. wsparcie dla SNMP, IPMI2.0, SSH, Redfish
    14. możliwość zdalnego monitorowania w czasie rzeczywistym oraz historycznym min 24h poboru mocy oraz temperatur w serwerze
    15. możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer
    16. integrację z Active Directory
    17. możliwość zdefiniowania minimum 12 użytkowników lokalnych na karcie zarządzającej
    18. możliwość obsługi zdalnej konsoli przez minimum czterech administratorów jednocześnie
    19. wsparcie dla dynamic DNS
    20. możliwość podglądu stanu serwera poprzez port USB i aplikację na urządzenie mobilne Android/iOS
23. **Oprogramowanie do zarządzania** - dodatkowe oprogramowanie producenta do zarządzania, spełniającego poniższe wymagania:
    1. Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych
    2. integracja z Active Directory
    3. Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta w systemie operacyjnym
    4. Automatyczne rozpoznawanie nowych serwerów poprzez protokół SLP oraz SSDP
    5. Szczegółowy opis wykrytych systemów oraz ich komponentów
    6. Możliwość eksportu danych minimum do formatu CSV
    7. Grupowanie urządzeń w oparciu o kryteria użytkownika
    8. Możliwość wizualizacji rozmieszczenia serwerów i zarządzanych urządzeń w szafach RACK
    9. Tworzenie automatycznie grup urządzeń w oparciu o elementy konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji czy stanu np. firmware czy BIOS
    10. Szybki podgląd stanu środowiska
    11. Podsumowanie stanu dla każdego urządzenia
    12. Szczegółowy status urządzenia/elementu/komponentu
    13. Filtry raportów umożliwiające podgląd najważniejszych zdarzeń
    14. Integracja z service desk producenta dostarczonej platformy sprzętowej, pozwalając min weryfikacje statusu i dosyłanie paczek diagnostycznych
    15. Możliwość przejęcia zdalnego pulpitu
    16. Możliwość zamontowania wirtualnego napędu
    17. Kreator umożliwiający dostosowanie akcji dla wybranych alertów
    18. Przesyłanie alertów „as-is” do innych konsol firm trzecich
    19. Możliwość definiowania ról administratorów
    20. Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów
    21. Aktualizacja oparta o repozytorium aktualizacji – budowanie repozytorium w sposób automatyczny ze stron producenta
    22. Możliwość definiowania polityk aktualizacji (konkretne wersje firmware)
    23. Automatyczna polityka aktualizacji „Najnowsze dostępne”
    24. Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta na systemie operacyjnym
    25. Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
    26. Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta
    27. Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności czy powielania konfiguracji na inne serwery czy backup aktualnej konfiguracji
    28. Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile
    29. Wykonanie restartu serwera i automatyczne wejście do BIOSu/UEFI
    30. Zdalne bezpieczne usunięcie danych na dyskach SSD/HDD w serwerach
    31. Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym
    32. Integracja z środowiskiem VMware vCenter pozwalająca z konsoli/plugin:
24. wykonać zautomatyzowaną aktualizację firmware serwerów w clustrze Vmware do zdefiniowanej polityki poziomu mikrokodów
25. wykonać/zweryfikować konfigurację serwera zgodną ze zdefiniowaną polityka konfiguracji
26. z konsoli vCenter uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny)
27. z konsoli vCenter uruchomić
28. inwentaryzacja komponentów w serwerze i ich mikrokodów
29. historia min 24h poboru mocy i temperatury serwera
30. zbieranie danych diagnostycznych serwera do paczki
    1. Integracja z środowiskiem Microsoft Admin Center pozwalająca z konsoli/plugin:
31. wykonać zautomatyzowaną aktualizację firmware serwerów w clustrze do zdefiniowanej polityki poziomu mikrokodów
32. z konsoli Admin Center uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny)
33. aktualizacja sterowników systemowych Windows
34. inwentaryzacja komponentów w serwerze i ich mikrokodów
35. historia min 24h poboru mocy i temperatury serwera
36. zbieranie danych diagnostycznych serwera do paczki
    1. Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V
37. **Certyfikaty**
    1. Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001
    2. Serwer musi posiadać deklarację CE.
    3. Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć.
    4. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC.
    5. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Bronze według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu.
    6. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
38. **Dokumentacja użytkownika**
    1. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
    2. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
39. **Warunki gwarancji**
    1. 60 miesięcy gwarancji producenta
    2. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24x7 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.
    3. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta powinien zakończyć naprawę minimum 24h od zakończenia diagnostyki zdalnej. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.
    4. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy.
    5. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.
    6. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon/aplikacja/ portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.
    7. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.
    8. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników.
    9. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii.
    10. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych.
    11. Możliwość rozszerzenia gwarancji przez producenta do 7 lat.
    12. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – na żądanie Zamawiającego przed podpisaniem Umowy.
    13. Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
    14. Uszkodzone dyski pozostają własnością Zamawiającego.

**III. CENTRALNA STACJA ZARZĄDZAJĄCA – 1 sztuka** (wymagania minimalne)

1. **Procesor**
   1. stacja wyposażona w procesor wielordzeniowy, wysokonapięciowy ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach przenośnych klasy x86, o parametrach minimum 26000 punktów na podstawie testu CrossMarkOverall Performance (min. v 1.0.1.88).
   2. Testy wykonane przy standardowych ustawieniach oprogramowania testującego w środowisku MS Windows 11 Professional 64-bit w aktualnej wersji.
   3. Procesor wyposażony w dedykowany układ do przetwarzania funkcjonalności sztucznej inteligencji (NPU) o wydajności min. 10 TOPS.
2. **Pamięć operacyjna RAM**
   1. Minimum 64 GB LPCAMM2 pracującej w trybie dual channel.
   2. Możliwość rozbudowy pamięci do minimum 64GB.
3. **Parametry pamięci masowej**
   1. Minimum 2 dyski M.2 SSD PCIe NVMe Performence o łącznej pojemności 2TB.
   2. Dysk samoszyfrujący w technologii OPAL 2.0
4. **Karta graficzna**
   1. Dedykowana do zastosowań profesjonalnych, zaprojektowana do pracy w mobilnych stacjach roboczych oraz posiadająca minimum 8GB własnej pamięci niewspółdzielonej w standardzie GDDR6.
   2. Pobór mocy (TGP) układu graficznego nieprzekraczający 60W.
   3. Karta graficzna osiągająca wynik minimum17000 punktów w teście PassMark - G3D Mark przy standardowych ustawieniach oprogramowania testującego w środowisku MS Windows 11 Professional 64-bit w aktualnej wersji.
5. **Obudowa** - Wykonana z metali lekkich lub kompozytów (np. aluminium, duraluminium, włókno węglowe, włókno szklane, PC-ABS) charakteryzujących się podwyższoną odpornością na uszkodzenia mechaniczne oraz przystosowana do pracy w trudnych warunkach termicznych. Komputer spełniający normy MIL-STD-810H.
6. **Waga** - Startowa waga urządzenia nieprzekraczająca 1,9 kg według karty katalogowej producenta.
7. **Ekran** - Matowy, matryca IPS 16”, rozdzielczość min. WQXGA (2560x1600), min. 500 nitów, kontrast 1200:1, gamut sRGB min. 100%. Kąt otwarcia pokrywy ekranu min. 180 stopni
8. **Karta sieciowa WLAN**
9. Wi-Fi 7
10. Bluetooth minimum 5.4
11. **Klawiatura -** odporna na zalanie cieczą, układ US, klawiatura wyposażona w minimum dwu stopniowe podświetlanie przycisków (włączone, wyłączone).
12. **Akumulator** - O pojemności min. 85Wh, obsługujący funkcjonalność szybkiego ładowania od 0 do 80% w czasie 60 minut lub od 0 do 50% w czasie 30 minut.
13. **Zasilacz zewnętrzny** - minimum 135W, wyprodukowany przez producenta komputera, dedykowany do oferowanego modelu.
14. **Stacja dokująca** - pochodząca od tego samego producenta, dedykowana do obsługi mobilnych stacji roboczych (300W)
15. **Certyfikaty, oświadczenia i standardy**
    1. dla producenta sprzętu należy dostarczyć certyfikat:
       1. ISO 9001
       2. ISO 14001
       3. ISO 50001
    2. dla komputera należy dostarczyć certyfikat:
       1. EPEAT Gold dla kraju Polska według danych widocznych na stronie <https://epeat.net/search-computers-and-displays>
       2. TCO 9.0 potwierdzone wpisem na stronie: <https://tcocertified.com/product-finder/>
       3. MIL-STD-810H
       4. Deklaracja zgodności CE
16. **System operacyjny** - Microsoft Windows 11 Pro 64 bit lub system operacyjny klasy PC, który spełnia następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:
    1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
       1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy.
       2. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych.
       3. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego.
       4. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim.
       5. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.
       6. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe.
       7. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych.
       8. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.
       9. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim.
       10. Wbudowany system pomocy w języku polskim.
       11. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).
       12. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.
       13. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.
       14. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.
       15. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
       16. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.
       17. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".
       18. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.
       19. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.
       20. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.
       21. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.
       22. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.
       23. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.
       24. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).
       25. Wbudowany mechanizm wirtualizacji typu hypervisor.
       26. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.
       27. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.
       28. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.
       29. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do minimum 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).
       30. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi.
       31. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.
       32. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.
       33. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM.
       34. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.
       35. Możliwość tworzenia wirtualnych kart inteligentnych.
       36. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot).
       37. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.
       38. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.
       39. Mechanizmy logowania w oparciu o:
17. Login i hasło,
18. Karty inteligentne i certyfikaty (smartcard),
19. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
20. Certyfikat/Klucz i PIN
21. Certyfikat/Klucz i uwierzytelnienie biometryczne
    * 1. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5
      2. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.
      3. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach
      4. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń
      5. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń
22. **Gwarancja i wsparcie techniczne producenta**
    1. Minimum 60 miesięcy gwarancji świadczonej w miejscu użytkowania sprzętu (on-site).
    2. Zgłoszenia serwisowe nadzorowane przez dedykowanych koordynatorów technicznych.
    3. Typ gwarancji umożliwiający priorytetyzację dostawy części zamiennych.
    4. Pomoc techniczna dostępna 24 godziny na dobę przez 365 dni w roku.
    5. Firma serwisująca posiadająca certyfikat ISO 9001:2000 na świadczenie usług serwisowych.
    6. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.
    7. Dedykowany portal techniczny producenta komputera, wyposażony w funkcję automatycznej identyfikacji urządzenia, umożliwiający Zamawiającemu uzyskanie informacji w zakresie co najmniej:
23. fabrycznej konfiguracji urządzenia,
24. rodzaju gwarancji,
25. dacie wygaśnięcia gwarancji,
26. aktualizacjach.
    1. Zaawansowana diagnostyka urządzenia i oprogramowania dostępna na stronie producenta komputera.

**IV. PRZEŁĄCZNIKI SIECIOWE – 4 sztuki -** wymagania:

1. **Rodzaj przełącznika -** Przełącznik musi być wykonany w technologii FC minimum 64 Gb/s i zapewniać możliwość pracy portów FC z prędkościami 64, 32, 16, oraz 8 Gb/s w zależności od rodzaju zastosowanych wkładek SFP+
2. **Wydajność**
   1. Wszystkie zaoferowane porty przełącznika FC muszą umożliwiać działanie bez tzw. oversubscrypcji, gdzie wszystkie porty w maksymalnie rozbudowanej konfiguracji przełącznika mogą pracować równocześnie z pełną prędkością 64 Gb/s.
   2. Całkowita przepustowość przełącznika FC musi wynosić minimum 4 Tb/s.
   3. Oczekiwana wartość opóźnienia przy przesyłaniu ramek FC między portami przełącznika nie może być większa niż 500 ns.
3. **Ilość portów**
   1. Przełącznik FC musi posiadać minimum 56 portów FC z czego minimum 24 aktywne porty FC obsadzone wkładkami o prędkości minimum 22 wkładkami 32 Gb/s SFP+ SWL i 2 wkładkami 32 Gb/s SFP+ LWL.
   2. Przełącznik musi umożliwiać zastosowanie wkładek podwójnej gęstości dla zwiększenia ilości portów do 64.
   3. Przełącznik musi również umożliwiać obsługę portów FC z prędkością 10 Gb/s.
4. **Rodzaj obsługiwanych portów** - co najmniej: E, F, Diagnostic Port
5. **Kable optyczne** - wraz z przełącznikiem musi zostać dostarczonych 48 kabli optycznych LC-LC klasy OM4 o długości 5m
6. **Typ obudowy** - przełącznik FC musi być przystosowany do montażu w szafie typu rack 19”, o wysokości maksymalnie 1U
7. **Zasilanie**
   1. Maksymalny dopuszczalny pobór mocy przełącznika FC w maksymalnej konfiguracji 64 porty 64 Gb/s SW nie może wynosić więcej niż 350W.
   2. Maksymalna ilość ciepła wydzielanego przez przełącznik FC w maksymalnej konfiguracji 64 porty 64 Gb/s SW nie może przekraczać 1200 BTU na godzinę.
8. **Agregacja połączeń**
   1. Przełącznik FC musi posiadać mechanizm agregacji połączeń ISL między dwoma przełącznikami i tworzenia w ten sposób logicznych połączeń typu ISL Trunk o przepustowości minimum 512 Gb/s złożony z niemniej niż 8 połączeń.
   2. Load balancing ruchu między fizycznymi połączeniami ISL w ramach połączenia logicznego typu trunk musi być realizowany na poziomie pojedynczych ramek FC, a połączenie logiczne musi zachowywać kolejność przesyłanych ramek.
   3. Jeżeli funkcjonalność jest licencjonowana należy dostarczyć licencje na maksymalną konfigurację przełącznika.
9. **Agregacja i balansowanie ruchem**
   1. Przełącznik FC musi wspierać mechanizm balansowania ruchu pomiędzy co najmniej 16 różnymi połączeniami o tym samym koszcie wewnątrz wielodomenowych sieci fabric, przy czym balansowanie ruchu musi odbywać się w oparciu o trzy parametry nagłówka ramki FC: DID, SID i OXID.
   2. Przełącznik FC musi zapewniać jednoczesną obsługę mechanizmów ISL Trunk oraz balansowania ruchu w oparciu o DID/SID/OXID.
   3. Jeżeli funkcjonalność jest licencjonowana należy dostarczyć licencje na maksymalną konfigurację przełącznika
10. **Zoning -** przełącznik FC musi realizować sprzętową obsługę zoningu (przez tzw. układ ASIC) na podstawie portów i adresów WWN
11. **Aktualizacja oprogramowania -** przełącznik FC musi mieć możliwość wymiany i aktywacji wersji firmware’u (zarówno na wyższą wersję jak i niższą) w czasie pracy urządzenia i bez zakłócenia przesyłanego ruchu FC
12. **Bezpieczeństwo -** przełącznik FC musi wspierać mechanizmy zwiększające poziom bezpieczeństwa:
    1. uwierzytelnianie przełączników w sieci fabric za pomocą protokołów DH-CHAP i FCAP;
    2. mechanizm tzw. Fabric Binding, który umożliwia zdefiniowanie listy kontroli dostępu regulującej prawa przełączników FC do uczestnictwa w sieci fabric;
    3. uwierzytelnianie urządzeń końcowych w sieci fabric za pomocą protokołu DH-CHAP;
    4. szyfrowanie połączenia z konsolą administracyjną (wsparcie dla SSHv2);
    5. definiowanie wielu kont administratorów z możliwością ograniczenia ich uprawnień za pomocą mechanizmu tzw. RBAC (Role Based Access Control);
    6. definiowane kont administratorów w środowisku RADIUS i LDAP w MS Active Directory, Open LDAP, TACACS+;
    7. szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS;
    8. obsługa minimum SNMP v3;
    9. IP Filter dla portu administracyjnego przełącznika;
    10. wgrywanie nowych wersji firmware przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP;
    11. wykonywanie kopii bezpieczeństwa konfiguracji przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP.
13. **Sposób zarządzania**
    1. Przełącznik FC musi mieć możliwość konfiguracji przez polecenia tekstowe w interfejsie znakowym konsoli terminala oraz przeglądarkę internetową z interfejsem graficznym lub dedykowane oprogramowanie.
    2. Interfejs graficzny oprogramowanie musi umożliwiać podstawową konfiguracje przełącznika, diagnostykę połączeń, konfiguracje portów, konfiguracje połączeń pomiędzy hostami a macierzami, analiza błędów ramek, wszystkich połączeń FC, które obsługuje przełącznik, tworzenie użytkowników, wykonywanie kopii konfiguracji przełącznika.
14. **Diagnostyka i analiza ruchu FC** - przełącznik FC musi wspierać następujące narzędzia diagnostyczne i mechanizmy obsługi ruchu FC:
    1. logowanie zdarzeń poprzez mechanizm „syslog”
    2. ciągłe monitorowanie parametrów pracy przełącznika, portów, wkładek SFP i sieci fabric z automatycznym powiadamianiem administratora (e-mail), wyłączeniem pracy portu lub przesunięciem przepływów tzw. slow drain na niski priorytet w przypadku przekroczenia zdefiniowanych wartości granicznych
    3. port diagnostyczny tzw. D\_port, który umożliwia wykonanie testów sprawdzających komunikację portu przełącznika z wkładką SFP, połączenie optyczne pomiędzy dwoma przełącznikami, testowe obciążenie połączenia pełną przepustowością oraz pomiar opóźnienia i odległości między przełącznikami (testy wykonywane przez port diagnostyczny nie mogą wpływać w żaden sposób na działanie pozostałych portów przełącznika i całej sieci fabric)
    4. FCping
    5. FC traceroute
    6. kopiowanie danych wymienianych pomiędzy dwoma wybranymi portami na inny wybrany port przełącznika
    7. mechanizm sprzętowego monitorowania przepływów danych dla wskazanych jak i automatycznie wykrywanych par urządzeń komunikujących się przez dany port przełącznika
    8. mechanizm sprzętowego generatora ruchu umożliwiającego symulowanie komunikacji w wielodomenowych sieciach SAN bez konieczności angażowania fizycznych urządzeń takich jak serwery lub macierze dyskowe
    9. mechanizm umożliwiający kopiowanie pierwszych 64 bajtów ramek dla wybranych przepływów danych do pamięci lokalnej przełącznika w celu dalszej analizy
    10. mechanizm umożliwiający sprzętowe identyfikowanie ramek FC oznaczonych parametrem VM ID oraz integrację tego mechanizmu z systemami monitorowania przepływów danych w szczególności w zakresie przepustowości, liczby zapisów i odczytów na sekundę oraz opóźnień operacji zapisu i odczytu.

Jeżeli w/w funkcjonalności są licencjonowana należy dostarczyć licencje na maksymalną konfigurację przełącznika.

1. **Dostęp -** przełącznik FCmusi posiadać zarządzanie przez zintegrowany port Ethernet, port szeregowy oraz inband IP-over-FC.
2. **Wsparcie REST API-** przełącznik FC musi zapewniać obsługę interfejsu zarządzającego REST API.
3. **Obsługa NVMe -** przełącznik FC musi zapewniać obsługę protokołu NVMe over FC.
4. **Kategoryzacja ruchu**
   1. Przełącznik FC musi realizować kategoryzację ruchu między parami urządzeń (initiator - target) oraz przydzielenie takich par urządzeń do kategorii o wysokim, średnim lub niskim priorytecie.
   2. Konfiguracja przydziału do różnych klas priorytetów musi się odbywać za pomocą standardowych narzędzi do konfiguracji zoningu.
   3. Przełącznik FC musi realizować kategoryzację ruchu na podstawie wartości parametru CS\_CTL w nagłówku ramki FC oraz odpowiednie przydzielenie ramki do kategorii o wysokim, średnim lub niskim priorytecie.
5. **Obsługa NPIV**
   1. Wsparcie dla N\_Port ID Virtualization (NPIV).
   2. Obsługa, co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika
6. **Gwarancja**
   1. Gwarancja producenta na okres 60 miesięcy w miejscu instalacji.
   2. Możliwość zgłoszenia awarii przez 24 godziny na dobę.
   3. Czas reakcji tego samego dnia.
   4. W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z przełącznikiem oraz oprogramowania wewnętrznego przełącznika. Serwis musi być realizowany przez producenta przełącznika w języku polskim.

**V. SZAFA SERWEROWA – 1 sztuka -** 42 U przystosowana do instalacji sprzętu 19” zgodnie ze standardem EIA-310-E, wraz z wyposażeniem

1. **Wymagania techniczne**
   1. Maksymalna wysokość 200 cm
   2. Szerokość minimalna 60 cm
   3. Maksymalna głębokość 120 cm
   4. Nośność (obciążenie statyczne) minimum 950 kg
   5. Wysokość w szafie przemysłowej 42U
   6. Kolor: czarny
   7. Drzwi przednie perforowane, zamykane na klamkę z kluczykiem
   8. Drzwi tylne perforowane, dzielone, zamykane na klamkę z kluczykiem
   9. Zdejmowane panele boczne
   10. Szafa dostarczona w stanie złożonym
   11. Zintegrowane uziemienie elektryczne:
2. Połączenia uziemiające na drzwiach
3. Dach, panele boczne, drzwi są uziemione do ramy
4. Dodatkowe zewnętrzne miejsca uziemienia z przodu / z tyłu
   1. Nóżka poziomująca, sprzęt mocujący, wstępnie zainstalowane kółka samonastawne
   2. Wyprodukowana przez producenta serwerów dostarczanych w ramach postępowania
   3. Okres gwarancji nie mniej niż 36 miesięcy
5. **Wyposażenie – PDU kompatybilne z oferowaną szafą rack** **– 2 sztuki**
   1. Minimalne wymagania techniczne dla jednostki PDU:
      1. Jednostka do montażu w szafie rack
      2. Temperatura eksploatacji -5 - 60 °C
      3. Wilgotność względna podczas pracy 5 - 95 %
   2. Parametry wejściowe:
      1. Nominalne napięcie wejściowe 400V 3PH
      2. Typ gniazda wejściowego: - IEC309 32A 3P+N+PE
      3. Maksymalny prąd na wejściowy: 32A
   3. Parametry wyjściowe:
      1. Napięcie wyjściowe 230VAC
      2. Złącza/gniazda wyjściowe 24 x C19 i 24 x C13
   4. Parametry:
      1. Wysokość: max.1500mm
      2. Szerokość: max 60mm
      3. Głębokość max 80mm
      4. Kolor: czarny
   5. Gwarancja: 36 miesięcy

**VI. USŁUGI WDROŻENIOWE**

1. Migracja aktualnej sieci san na nowe przełączniki sieci SAN (dwie lokalizacje oddalone o około 0,5km - aktualnie sieć używa 4 linki fc między dwoma lokalizacjami na światłowodzie SM –pozostała cześć środowiska działa na wkładkach multimodowych)
2. Konfiguracja klastra active/active na dwóch macierzach oraz na przełącznikach sieci SAN
3. Migracja danych z aktualnych macierzy na klaster złożony z dwóch nowych macierzy
4. Aktualizacji posiadanego oprogramowania Vmware do aktualnie najnowszej, wspieranej wersji (licencje dostarcza Zamawiający)
5. Wszystkie prace muszą zostać wykonane bezprzerwowo dla maszyn wirtualnych vSphere
6. Zamawiający nie dopuszcza pracy zdalnej, wszystkie prace należy wykonać w siedzibie Zamawiającego
7. Wszystkie prace uwzględniają transport do dwóch serwerowni, instalacje, okablowanie, oznakowanie naklejkami kabli i sprzętu, konfiguracje, zabranie opakowań po sprzęcie
8. Zastąpienie dwóch wskazanych przez Zamawiającego serwerów obecnie będących częścią farmy Vmware Vsphere, dostarczonym sprzętem
9. Dostarczenie, instalacja i konfiguracja wszystkie komponentów zgodnie z ustaleniami z Zamawiającym.
10. Instalacja szafy rack w pomieszczeniu wskazanych przez Zamawiającego
11. Dostarczenie wszelkich niezbędnych elementów do wykonania prac w szczególności kabli elektrycznych, światłowodów, kabli Ethernet kat. 6e, modułów PDU do szafy rack, itp. w ilości oraz długości pozwalającej na prawidłowe podłączenie wszystkich urządzeń dostarczanych w ramach postępowania
12. Prace obejmują podłączenie wszystkich oferowanych rozwiązań do sieci LAN i SAN Zamawiającego
13. Montaż całości sprzętu w szafach RACK w pomieszczeniach wskazanych przez Zamawiającego
14. Ułożenie okablowania instalowanego sprzętu w przeznaczonych do tego celu korytkach, organizerach okablowania, szufladach zapasu itp.
15. Aktualizacja oprogramowania układowego (firmware, BIOS) wszystkich dostarczonych urządzeń do najnowszych stabilnych wersji.
16. Wykonawca opracuje szczegółową dokumentację techniczną powykonawczą zawierającą dokładny opis montażu, instalacji i konfiguracji zainstalowanych komponentów sprzętowych i oprogramowania. Dokumenty będą dostarczone Zamawiającemu w języku polskim, w wersji elektronicznej, edytowalnej (plik MS Word 2016) a także w wersji Portable Document Format (zgodny z ISO 32000-1:2008) oraz w formie wydruku.
17. Wykonawca przeprowadzi testy sprawdzające niezawodność na wypadek awarii pojedynczego punktu infrastruktury według scenariuszy przygotowanych przez Wykonawcę i zatwierdzonych przez Zamawiającego.

**VII. WSPARCIE TECHNICZNE**

1. **Zakres wsparcia technicznego obejmuje:**
   1. usuwanie awarii (krytycznych i niekrytycznych),
   2. rozwiązywanie problemów z dostarczonym sprzętem w celu zapewnienia ciągłości pracy środowiska serwerowo - sieciowego Zamawiającego,
   3. rekonfigurację urządzeń zgodnie z wymaganiami Zamawiającego,
   4. aktualizację oprogramowania na dostarczonych przez Wykonawcę urządzeniach,
   5. uaktualnienia oraz instalację oprogramowania firmware nie rzadziej niż raz na 180 dni w siedzibie Zamawiającego, jeżeli takie uaktualnienia są rekomendowane przez producenta urządzeń i/lub oprogramowania
   6. komunikacja z Wykonawcą dotycząca usługi wsparcia odbywać się będzie za pośrednictwem dedykowanych kanałów komunikacji: telefon lub e-mail
   7. minimum raz na kwartał przegląd zakupionych urządzeń, potwierdzony przez Zamawiającego
   8. w przypadku awarii dostarczonych urządzeń i oprogramowania wsparcie między serwisem producenta a Zamawiającym
   9. uszkodzone dyski stanowią własność Zamawiającego i nie podlegają zwrotowi w ramach usługi gwarancyjnej i/lub usługi wsparcia technicznego
2. **Czas trwania usługi wsparcia technicznego** – 36 miesięcy
3. **Zakres czasowy usługi wsparcia:**
   1. 8 godzin w miesiącu (godziny niewykorzystane w danym miesiącu przechodzą na kolejne okresy)
   2. Przyjmowanie zgłoszeń serwisowych 24 godziny przez 7 dni w tygodniu z czasem reakcji (potwierdzenie przyjęcia zgłoszenia) w ciągu 1 godziny
4. **Czas reakcji**:
   1. zgłoszenia krytyczne - (zdarzenie, awaria uniemożliwiająca pracę systemu bądź powodująca znaczne straty finansowe Zamawiającego) - nie dłużej niż 4 godziny licząc od momentu zgłoszenia do czasu przybycia do siedziby Zamawiającego, celem podjęcia koniecznych prac naprawczych
   2. zgłoszenia niekrytyczne - (zdarzenie, usterka utrudniająca pracę systemu) - w następnym dniu roboczym (od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy) licząc od chwili zgłoszenia wystąpienia awarii lub usterki, z zastrzeżeniem, że zgłoszenia dokonano nie później niż do godz. 17:00

**Załącznik nr 9** – Klauzula Informacyjna

Nr sprawy: **ZR-078/D/RZ/2024**

Zamówienie pn. „*Zakup i instalacja macierzy i serwerów*”

ZAMAWIAJACY: **Miejskie Wodociągi i Kanalizacja w Bydgoszczy - spółka z o.o.**

**KLAUZULA INFORMACYJNA ADMINISTRATORA**

**W ZWIĄZKU Z PRZETWARZANIEM DANYCH OSOBOWYCH**

Zgodnie z art. 13 ust. 1 i ust. 2 oraz art. 14 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE* (dalej jako: „**RODO**”), poniżej Zamawiający informuje o przetwarzaniu danych osobowych w związku z prowadzonym postępowaniem zakupowym oraz zasadach, na jakich będzie się to odbywało.

1. Administratorem danych osobowych osób, których dane zostają przekazane Zamawiającemu przez wykonawców w związku z ubieganiem się przez wykonawców o udzielenie zamówienia są: Miejskie Wodociągi i Kanalizacja w Bydgoszczy sp. z o.o., ul. Toruńska 103, 85-817 Bydgoszcz.
2. Zamawiający wyznaczył Inspektora Ochrony Danych, z którym można się kontaktować poprzez e-mail: [wojciechowski@mwik.bydgoszcz.pl](mailto:wojciechowski@mwik.bydgoszcz.pl) lub pod nr telefonu 693-168-329.
3. Dane osobowe przekazane Zamawiającemu są przetwarzane w celu przeprowadzenia postępowania oraz dokonania wyboru najkorzystniejszej oferty. Dane osobowe mogą być także przetwarzane w celu zawarcia umowy z wybranym wykonawcą oraz właściwego rozliczenia sposobu wydatkowania środków uzyskanych na sfinansowanie zamówienia.
4. Dane osobowe są przetwarzane na następujących podstawach:

* dla wypełnienia obowiązku prawnego ciążącego na Zamawiającym (art. 6 ust. 1 lit. c RODO) lub wykonywania zadań realizowanych w interesie publicznym (art. 6 ust. 1 lit. e RODO);
* dla realizacji prawnie uzasadnionego interesu Zamawiającego tj. w celu poprawnego przygotowania oraz przeprowadzenia postępowania o udzielenie zamówienia, jak również w celu prawidłowego wydatkowania środków uzyskanych na sfinansowanie zamówienia (art. 6 ust. 1 lit. f RODO);
* dla wypełnienia zobowiązań umownych (art. 6 ust. 1 lit. b RODO – w przypadku, gdy wykonawca jest osobą fizyczną lub prowadzi jednoosobową działalność gospodarczą).

1. Odbiorcami danych osobowych będą upoważnieni pracownicy Zamawiającego odpowiedzialni za przygotowanie i przeprowadzenie postępowania o udzielenie zamówienia oraz podmioty realizujące usługi na rzecz Zamawiającego (np. usługi IT, doradztwo prawne). Odbiorcami danych mogą być również osoby lub podmioty, którym zostanie udostępniona dokumentacja postępowania (w szczególności w zakresie i na zasadach określonych w obowiązującym u Zamawiającego regulaminie udzielania zamówień) oraz podmioty kontrolujące wydatkowanie uzyskanych przez Zamawiającego środków finansowych.
2. Dane osobowe będą przetwarzane przez okres niezbędny do przeprowadzenia postępowania i dokonania wyboru najkorzystniejszej oferty. Po tym okresie, dane mogą być przetwarzane przez okres realizacji zamówienia, a po tym czasie w ramach obowiązków prawnych Zamawiającego lub dla realizacji jego uzasadnionego interesu np. z uwagi na obowiązujące terminy kontroli przeprowadzanej w zakresie właściwego wydatkowania przez Zamawiającego środków pozyskanych na sfinansowanie niniejszego zamówienia.
3. Podanie danych osobowych jest dobrowolne, jednak może być niezbędne dla wzięcia udziału w postępowaniu.
4. Osobie, której dane są przetwarzane, przysługuje: prawo dostępu do danych osobowych, ich sprostowania, usunięcia, ograniczenia przetwarzania danych osobowych oraz wniesienia sprzeciwu wobec przetwarzania (gdy dane są przetwarzane na podstawie art. 6 ust. 1 lit. e lub f RODO). W razie uznania, że doszło do naruszenia ochrony danych, osobie, której dane są przetwarzane, przysługuje prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
5. Administrator przetwarza następujące kategorie danych osobowych, których nie uzyskał bezpośrednio od osoby, której dane dotyczą (np. dane osoby skierowanej do realizacji zamówienia, podwykonawcy, pełnomocnika, członka organu), w zależności od potrzeb: imiona i nazwiska, imiona rodziców, miejsce i datę urodzenia, obywatelstwo, adres zamieszkania, adres korespondencyjny, PESEL, NIP, serię i numer dokumentu potwierdzającego tożsamość, datę jego wydania oraz datę ważności dokumentu, podmiot wydający dokument; numer telefonu komórkowego, adres poczty elektronicznej, miejsce pracy, stanowisko, uprawnienia.
6. Zamawiający uzyskał dane osobowe bezpośrednio od wykonawcy lub z publicznie dostępnych rejestrów.
7. Wykonawca jest zobowiązany do poinformowania osób, których dane przekazuje, o sposobie przetwarzania ich danych przez Zamawiającego, zgodnie z pkt. 1-10 powyżej.