Załącznik nr 1.1 do SIWZ

Szczegółowy opis przedmiotu zamówienia

dla zamówienia na dostawa platformy serwerowej, systemu backupu, macierzy dyskowych, urządzeń sieciowych na potrzeby projektu pn.: „Śląskie Digitarium. Digitalizacja i udostępnianie zasobów instytucji kultury województwa śląskiego”

Część 1 - Serwery, macierze, urządzenia sieciowe, backup dla Biblioteki Śląskiej w Katowicach

Katowice, dnia 22.12.2020r.

I. SŁOWNIK TERMINÓW

W opisie przedmiotu zamówienia używane są następujące terminy, pojęcia i skróty:

Pojemność katalogowa vs pojemność logiczna pamięci masowych:

- **1TB** = 10^{12} bajtów – terabajt – jednostka pojemności będzie używana w odniesieniu do pojemności katalogowej (surowej) dysków twardych i pamięci flash; większość producentów podaje pojemność produkowanych modułów w terabajtach;
- **1TiB** = 2^{40} bajtów – tebibajt – jednostka pojemności będzie używana w odniesieniu do pojemności logicznej (użytkowej) macierzy dyskowych oraz macierzy obiektowych oraz systemu kopii zapasowych – po przeliczeniu pojemności jednostkowych katalogowych urządzeń składowych (dyski, moduły flash) oraz uwzględnieniu redundancji przechowywania danych (struktury RAID, Erasure Coding itd.).
- **Uwaga! 1 TiB = 1.099511627776 TB – zatem przy wyliczaniu pojemności użytkowej systemów należy uwzględnić ten fakt; wymagania dot. pojemności logiczna (użytkowa) macierzy dyskowych, macierzy obiektowych oraz systemu kopii zapasowych określone są w TB**

II. SPECYFIKACJA TECHNICZNA

OPIS KONCEPCYJNY INFRASTRUKTURY SERWEROWEJ

Infrastruktura serwerowa do długoterminowego zachowania i prezentacji zdigitalizowanych zbiorów piśmiennictwa i obiektów 3D Biblioteki Śląskiej w Katowicach, której zakup, dostawa, wdrożenie i serwisowanie jest przedmiotem niniejszego postępowania składa się z 5 głównych grup funkcjonalnych systemów IT rozmieszczonych w 2 centrach danych w budynkach Biblioteki Śląskiej w Katowicach.

Komponenty funkcjonalne i ich przeznaczenie

Komponenty funkcjonalne infrastruktury serwerowej obejmują:

1. **System wysokiej dostępności oraz system baz danych NoSQL** – systemy dla uruchamiania aplikacji i platform i narzędzi realizujących główną funkcjonalność infrastruktury i procesy biznesowe projektu, w zakresie pozyskiwania, zachowania i prezentacji zdigitalizowanych treści cyfowych; systemy te obejmują:
   a. **12** serwerów fizycznych – tzw. *system wysokiej dostępności* – wyposażonych w mechanizmy wirtualizacji, przeznaczone do uruchomienia **24** maszyn wirtualnych, głównie z systemami operacyjnymi Linux, w trybie wysokiej dostępności (minimum przełączanie obsługi maszyn wirtualnych między serwerami fizycznymi) – zawierających aplikacje, narzędzia, bazy danych i inne elementy przeznaczone do realizacji ścieżki digitalizacyjnej danych oraz długoterminowej archiwizacji danych, konwersji danych (np. PDF/OCR, zmiana formatów TIFF->JPG), prezentacji danych i serwowania treści (cyfrowa czytelnia, udostępnianie obrazów IIIF), a także indeksacji, agregacji i wyszukiwania meta-danych;
   b. **6** serwerów fizycznych – tzw. *System baz danych NoSQL* – opcjonalnie wyposażonych w mechanizmy wirtualizacji i wysokiej dostępności, przeznaczonych do uruchomienia 6 węzłów klastra NoSQL, w oparciu o systemy operacyjne z Linux; bazy danych NoSQL stanowią bazę dla systemu „agregator";
2. **Macierz dyskowa (centralna)** – dostarcza przestrzeń roboczą na pamięciach flash i dyskach magnetycznych dla danych systemowych maszyn wirtualnych oraz aplikacji i baz danych działających na serwerach; macierz świadczyć będzie usługi blokowe (FC) dla serwowania wolumenów dla maszyn wirtualnych w systemie wysokiej dostępności oraz opcjonalnie dla serwerów bazy danych NoSQL a także usługi plikowe (CIFS, NFS) – na potrzeby aplikacji i wymiany danych w ramach elementów infrastruktury serwerowej. *Dane składowane na macierzy zabezpieczone są poprzez redundantne składowanie w strukturach RAID oraz dodatkowo poprzez wykonywanie kopii zapasowych (za pośrednictwem platformy wirtualizacyjnej).*
3. **Macierze obiektowe** – zapewniające długofalowe, wiarygodne i odporne na awarie przechowywanie zdigitalizowanych zbiorów. Rozproszone geograficznie i zabezpieczone replikacją danych macierze obiektowe stanowić będą wysoko-pojemne i bezpieczne repozytorium zapewniające niezmienność zdeponowanych danych. Zabezpieczenie danych w macierzach obiektowych będą wielopoziomowe: lokalne składowanie redundantne danych (ang. *Erasure Coding)* oraz replikacja geograficzna. Macierze obiektowe udostępniać będą interfejsy obiektowe (minimum S3) i plikowe (minimum NFS). Macierze stanowić będą docelowe miejsce trwałego przechowywania zdigitalizowanych w infrastrukturze serwerowej danych.
4. **Sieć LAN i system UTM oraz sieć SAN dla infrastruktury serwerowej oraz sieć LAN pracowni i czytelni BŚ** – elementy sieci Ethernet (przełączniki), za pośrednictwem której stworzone zostaną połączenia wewnętrzne w ramach infrastruktury serwerowej oraz poprzez którą infrastruktura serwerowa zostanie podłączona do istniejącej sieci LAN Biblioteki Śląskiej oraz łączy WAN i sieci Internet; poprzez te sieci aplikacje i usługi infrastruktury serwerowej zostaną udostępnione uczestnikom projektu, w tym pracownikom lokalnym (za pośrednictwem sieci LAN dla pracowni i czytelni) oraz użytkownikom zewnętrznym; infrastruktura Ethernet obejmie także sieć zarządzającą dla serwerów, macierzy, systemu wykonywania kopii zapasowych, sieci LAN i SAN; ochrona zewnętrznego i wewnętrznego ruchu sieciowego zostanie zapewniona przez system UTM; z kolei sieć SAN zapewni podłączenie macierzy centralnej do serwerów systemu wysokiej dostępności i serwerów NoSQL oraz udostępnienie dla tych systemów przestrzeni przechowywania danych z macierzy centralnej; ponadto, elementy sieci LAN dla pracowni digitalizacyjnej i czytelni Biblioteki Śląskiej (przełączniki LAN) umożliwią podłączenie stacji roboczych zlokalizowanych w pomieszczeniach pracowni i czytelni do sieci LAN dla infrastruktury serwerowej, zapewniając odpowiednią wydajność dostępu do usług infrastruktury serwerowej z poziomu pracowni i czytelni Biblioteki Śląskiej;
5. **System wykonywania kopii zapasowych –** zabezpieczać będzie dane platformy wirtualizacyjnej, systemów operacyjnych i/lub wolumeny dyskowe maszyn wirtualnych, a także dane aplikacji, baz danych, platform i usług oraz dokumenty, obrazy, pliki tymczasowe i robocze użytkowników infrastruktury serwerowej przed awarią sprzętu i oprogramowania, błędami człowieka (operatora systemu, użytkownika) oraz złośliwym działaniem ludzi (np. sabotaż, ataki hakerów) lub oprogramowaniem (np. ang. *Ransomware*).

Wyżej opisane komponenty infrastruktury serwerowej stanowić będą bazę dla niezawodnej, bezpiecznej oraz wydajnej i efektywnej realizacji procesów związanych z długoterminowym zachowaniem i prezentacją zdigitalizowanych zbiorów piśmiennictwa i obiektów 3D Biblioteki Śląskiej. Ponadto komponenty te realizować będą funkcjonalność i usługi wspomagające realizację procesów w instytucjach współpracujących z Biblioteką Śląską w ramach projektu „Śląskie Digitarium. Digitalizacja i udostępnianie zasobów instytucji kultury województwa śląskiego", m.in. poprzez udostępnianie zasobów systemu przechowywania danych na potrzeby realizacji kopii zapasowych dla Opery Śląskiej. *Uzupełnieniem wymienionych wyżej komponentów jest system zasilania awaryjnego (UPS) będący przedmiotem oddzielnego zadania w ramach niniejszego postępowania.*

Rozmieszczenie elementów infrastruktury

Komponenty infrastruktury serwerowej do długoterminowego zachowania i prezentacji danych zostaną rozmieszczone w dwóch **centrach danych** Biblioteki Śląskiej:

1. **Centrum Podstawowe (CP)** – obejmujące serwerownię oraz pomieszczenie dla UPS i rozdzielni zlokalizowane w budynku Biblioteki Śląskiej na Placu Rady Europy 1 w Katowicach.
2. **Centrum Zapasowe (CZ)** – obejmujące serwerownię zlokalizowane w budynku Biblioteki Śląskiej przy ul. Ligonia 7 w Katowicach.

Lokalizacje te połączone są wydajną siecią w celu realizacji replikacji danych oraz awaryjnej obsługi dostępu do danych zgromadzonych w bezpiecznym archiwum obiektowym i/lub systemie wykonywania kopii zapasowych.

Elementy infrastruktury serwerowej do długoterminowego zachowania i prezentacji danych zostaną rozmieszczone w następujący sposób w serwerowniach (centrach danych) Biblioteki Śląskiej.

1. W serwerowni w Centrum Podstawowym umieszczone zostaną:
   - Serwery systemu wysokiej dostępności i serwery systemu baz danych NoSQL
   - Macierz dyskowa (centralna)
   - Macierz obiektowa (jedna z dwóch macierzy)
   - Elementy sieci LAN, system UTM i sieć SAN
   - System wykonywania kopii zapasowych (jedna z dwóch części systemu)

2. W serwerowni w Centrum Zapasowym umieszczone zostaną:
   - Macierz obiektowa (jedna z dwóch macierzy)
   - Elementy sieci LAN
   - System wykonywania kopii zapasowych (jedna z dwóch części systemu)

Ponadto w pomieszczeniach pracowni digitalizacyjnych i czytelni Biblioteki Śląskiej zostaną umieszczone elementy sieci LAN dla tych pracowni, tj. przełączniki łączące stacje robocze z infrastrukturą serwerową.

Poniższa tabela podsumowuje sposób rozmieszczenia elementów infrastruktura serwerowej w poszczególnych serwerowniach (centrach danych) Biblioteki Śląskiej:

Nazwa elementu	Centrum Podstawowe	Centrum Zapasowe
Serwery systemu wysokiej dostępności	TAK	NIE
Serwery systemu baz danych NoSQL	TAK	NIE
Macierz dyskowa (centralna)	TAK	NIE
Macierz obiektowa	TAK: Podstawowa kopia danych	TAK: Replika danych
Elementy sieci LAN	TAK	TAK
System UTM	TAK	NIE
Sieć SAN	TAK	NIE
System wykonywania kopii zapasowych	TAK: Podstawowa kopia zapasowa danych	TAK: Replika kopii zapasowej danych

Tabela 1 Rozmieszczenie elementów infrastruktury w serwerowniach

ZAKRES PRAC WYKONAWCY

Zakres prac wykonawcy w ramach realizacji dostawy i wdrożenia zaoferowanej infrastruktury serwerowej obejmuje zaprojektowanie, instalację, konfigurację, przeprowadzenie testów, wykonanie dokumentacji powykonawczej oraz przeprowadzenie instruktażu, w szczególności:

1. **Wykonanie szczegółowego projektu technicznego instalacji i konfiguracji infrastruktury serwerowej** – w ciągu 14 dni od momentu podpisania umowy – do akceptacji Zamawiającego (w ciągu 7 dni od przedłożenia); projekt musi obejmować minimum:
   a) Architekturę wdrożeniową sprzętu – w tym rozmieszczenie szaf serwerowych w serwerowniach, rozmieszczenie serwerów, macierzy, przełączników i innych elementów infrastruktury w szafach;
   b) Schemat przyłączenia sprzętu IT do zasilania – wraz ze schematem zabezpieczenia systemów komputerowych przed awarią zasilania – jeśli takie rozwiązanie jest dostarczane;
   c) Schemat połączeń sieciowych – zarówno dla sieci LAN produkcyjnej i zarządzającej oraz sieci SAN z uwzględnieniem połączeń z istniejącą infrastrukturą Biblioteki Śląskiej, włączając istniejącą sieć LAN, łącza WAN, połączenia między serwerowniami (Centrum Podstawowe i Centrum Zapasowe); ponadto schemat połączeń sieci LAN dla pracowni digitalizacyjnyj i czytelni biblioteki Śląskiej z siecią LAN produkcyjną dla infrastruktury serwerowej;
   d) Główne założenia konfiguracyjne sprzętu IT – w tym zdefiniowanie:
      a. Dla serwerów systemu wysokiej dostępności – listy maszyn wirtualnych, ich rozmieszczenie na hostach fizycznych, ich systemów operacyjnych, nazw w platformie wirtualizacyjnej, adresacji sieciowe oraz wykorzystywanych wolumenów dyskowych z macierzy centralnej;
      b. Dla serwerów systemu baz danych NoSQL – listy maszyn wirtualnych, ich rozmieszczenie na hostach fizycznych, ich systemów operacyjnych, nazw w platformie wirtualizacyjnej, adresacji sieciowej oraz wykorzystywanych dysków wewnętrznych *i opcjonalnie z macierzy centralnej*
      c. Dla macierz dyskowej (centralnej) – listy grup napędów flash (SSD/NVMe) i grup dysków magnetycznych (HDD) wraz z definicją struktur przechowywania redundantnego właściwych dla tych grup; listy wolumenów logicznych oraz mapowań wolumenów do serwerów i/lub grup serwerów systemu wysokiej dostępności i/lub serwerów systemu baz danych NoSQL; polityki wykonywania kopii zapasowych danych przechowywanych w macierzy;
      d. Dla sieci SAN – listy stref w sieci SAN (ang. *zone*) lub podsieci vSAN obejmujących (rozłączne) grupy serwerów systemu wysokiej dostępności i serwerów baz danych NoSQL
      e. Dla macierzy obiektowej – lista struktur redundantnych (puli dyskowych) oraz przykładowych/testowych przestrzeni/kontenerów/kont zapewniających minimum: (1) przestrzeń roboczą: składowanie i modyfikację danych i meta-danych oraz (2) przestrzeń archiwalną: składowanie danych w trybie WORM; konfiguracja/polityki retencji danych właściwe dla w/w wymienionych przestrzeni; konfiguracja mechanizmu replikacji danych pomiędzy Centrum Podstawowym i Centrum Zapasowym; konfiguracja mechanizmów wieloprotokołowego dostępu do przestrzeni (obiektowe: S3, plikowe – minimum NFS);
      f. Dla sieci LAN produkcyjnej i do zarządzania – listy sieci wirtualnych (VLAN i/lub VxLAN) wraz z listą serwerów i portów serwerów objętych tymi sieciami wirtualnymi;
      g. Dla systemu UTM – podstawowej (początkowej) listy polityk i głównych ustawień konfiguracyjnych dla mechanizmów ochrony ruchu sieciowego;
      h. Dla systemu wykonywania kopii zapasowych – podstawowej (początkowej) listy polityk kopii wykonywania kopii zapasowych środowiska wirtualizacyjnego oraz maszyn wirtualnych;
2. **Instalacja elementów infrastruktury serwerowej:**
   a) Transport, wniesienie do pomieszczeń serwerowni Biblioteki Śląskiej i instalacja szaf przemysłowych;
   b) Transport, wniesienie do pomieszczeń Biblioteki Śląskiej i instalacja w szafach systemów IT, sprawdzenie geometrii szaf po instalacji sprzętu, usunięcie opakowań sprzętu (nie dopuszcza się wykorzystania kontenerów na odpady Zamawiającego)
   c) Instalacja w szafach elementów systemu dystrybucji zasilania (PDU) oraz odpowiednie podłączenie PDU do systemu zasilania serwerowni, w sposób zapewniający spełnienie wymagań SIWZ;
   d) Instalacja, dystrybucja i ułożenie okablowania zgodnie z dobrymi praktykami – w tym okablowania zasilającego i komunikacyjnego, miedzianego i optycznego (m.in. zachowanie promieni gięcia) oraz w sposób zapewniający spełnienie wymagań SIWZ;
   e) Oznakowanie urządzeń i okablowania, za pomocą trwałych etykiet odpornych na działanie światłą, temperatury oraz podmuchów powietrza; w szczególności oznakowanie okablowania zasilającego podłączonego do różnych faz/źródeł zasilania odmiennymi kolorami etykiet;
3. **Konfiguracja infrastruktury serwerowej –** zgodnie z ustaloną konfiguracją wdrożeniową – obejmująca:
   a) Konfigurację serwerów systemu wysokiej dostępności, obejmująca minimum: instalację i konfigurację platformy wirtualizacyjnej, konfiguracja i aktywacja licencji na oprogramowanie wirtualizacyjne,

uruchomienie maszyn wirtualnych – minimum na bazie dostarczonych licencji na cztery instancje systemu operacyjnego Windows (instalacja, uruchomienie i aktywacja systemu) oraz minimum czterech instancji systemu operacyjnego z rodziny Linux (wersja uzgodniona z Zamawiającym);

b) Konfigurację serwerów systemu baz danych NoSQL: obejmująca minimum:
   a. jeśli zaoferowano platformę wirtualizacyjną dla tych serwerów – konfigurację tej platformy wirtualizacyjnej, w tym: instalację oprogramowania platformy wirtualizacyjnej, konfigurację i aktywację licencji na oprogramowanie wirtualizacyjne, uruchomienie maszyn wirtualnych; konfiguracja wolumenów na dyskach wewnętrznych serwerów systemu baz danych NoSQL;
   b. jeśli nie zaoferowano platformy wirtualizacyjnej dla tych serwerów: instalacja i uruchomienie systemów operacyjnych bezpośrednio na serwerach fizycznych systemu baz danych NoSQL; konfiguracja wolumenów na dyskach wewnętrznych serwerów systemu baz danych NoSQL;
c) Konfiguracja macierzy dyskowej (centralnej) – obejmująca minimum konfiguracja grup napędów flash (SSD/NVMe) i grup dysków magnetycznych (HDD) oraz struktur redundantnego przechowywania danych a także mapowań wolumenów flash i dyskowych do serwerów;
d) Dla sieci SAN – konfiguracja przełączników oraz stref sieci SAN (ang. zone) lub podsieci vSAN;
e) Dla sieci LAN – konfiguracja przełączników oraz sieci wirtualnych w ramach sieci LAN;
f) Dla systemu UTM – integracja z siecią LAN; konfiguracja polityk ochrony ruchu sieciowego LAN;
g) Dla systemu wykonywania kopii zapasowych – instalacja silnika wykonywania kopii zapasowych, definicja puli przechowywania danych oraz polityk wykonywania kopii zapasowych dla platformy wirtualizacyjnej a także systemów operacyjnych maszyn wirtualnych systemu wysokiej dostępności oraz serwerów systemu baz danych NoSQL (lub maszyn wirtualnych z systemem baz danych NoSQL); konfiguracja replikacji danych – mechanizmu zapewniającego *składowanie danych kopii zapasowej w obu serwerowniach Biblioteki Śląskiej – w Centrum Podstawowy oraz Centrum Zapasowym;*
h) *Konfiguracja mechanizmu automatycznego bezpiecznego wyłączania elementów infrastruktury serwerowej zapewniającego komunikację zasilaczy UPS dostarczanych do Centrum Podstawowego oraz Centrum Zapasowego Biblioteki Śląskiej z elementami infrastruktury serwerowej, w celu inicjacji procesu zamknięcia systemów operacyjnych, platform wirtualizacyjnych i aplikacji, zapisu buforów kontrolerów dyskowych, w tym RAID, w przypadku awarii zasilania przekraczającej zadany okres czasu (np. 5 minut); dostarczenie systemów UPS nie jest przedmiotem niniejszego zadania, jednak integracja wymaganych dla bezpiecznego wyłączania infrastruktury serwerowej musi być przeprowadzona przez Wykonawcę niniejszego zadania; w przypadku, gdy systemy UPS nie zostaną dostarczone i uruchomione w terminie realizacji niniejszego zadania, Wykonawca wymienioną powyżej konfigurację przeprowadzi w ramach czynności technicznych serwisu gwarancyjnego dla niniejszego zadania;*

4. **Dokumentacja:**
   a) Dostarczenie dokumentacji dla elementów infrastruktury serwerowej obejmującej minimum: schemat instalacji fizycznej, połączeń zasilających i komunikacyjnych a także konfigurację logiczną, w tym konfigurację platform wirtualizacyjnych dla serwerów systemu wysokiej dostępności oraz systemu baz danych NoSQL (jeśli dostarczono platformę wirtualizacyjną), konfigurację maszyn wirtualnych, systemów operacyjnych, dla sieci LAN adresacja sieciowa (adresy fizyczne/MAC i adresy IP) i podział na VLANy; konfigurację systemu UTM i polityk ochrony sieci; dla sieci SAN: adresy fizyczne/WWN i zdefiniowane strefy sieci; dla macierzy: konfigurację struktur redundantnego przechowywania danych (RAID oraz tzw. *Erasure Coding* i replikacja); zdefiniowane polityki zarządzania danymi w macierzach: buforowanie na pamięciach flash w macierzy centralnej, retencja danych w macierzy obiektowej, polityki replikacji geograficznej dla macierzy obiektowej; konfigurację; systemu wykonywania kopii zapasowych: polityki backup oraz replikacji danych;
   b) Dostarczenie kluczy licencyjnych, subskrypcji, certyfikatów dla licencji; instrukcji, kart katalogowych itp. w formie papierowej lub tam gdzie to możliwe elektronicznej na płycie CD/DVD oraz w postaci udostępnionego wskazanym do kontaktu pracownikom Biblioteki Śląskiej pliku z kopią tych danych;

5. **Instruktaż:**
   a) Instruktaż dotyczący podstawowych aspektów konfiguracyjnych i użytkownych zaoferowanego i wdrożonego sprzętu i oprogramowania, obejmujący minimum podstawową obsługę:
      a. systemu wysokiej dostępności oraz systemu baz danych NoSQL, platformy wirtualizacyjnej – tworzenie i konfigurację maszyn wirtualnych w ramach platformy wirtualizacyjnej, konfiguracja sieciowa serwerów fizycznych i maszyn wirtualnych, konfiguracja pamięci masowej dla serwerów fizycznych i maszyn wirtualnej (lokalnej i udostępnianej poprzez sieci SAN oraz protokoły plikowe (NFS, CIFS), monitoring serwerów fizycznych i maszyn wirtualnych; wykrywanie awarii oraz omówienie i demonstracja podstawowych czynności serwisowych, których wykonanie przez użytkownika zakłada się w zaoferowanym programie serwisowym (np. wymiana napędów flash lub dysków magnetycznych *hot-swap* w serwerach);

b. macierzy centralnej – tworzenie struktur redundantnego przechowywania danych (RAID), definiowanie hostów i mapowań wolumenów; konfiguracja buforowania wolumenów dyskowych z na pamięciach flash (SSD/NVMe); monitoring systemu w zakresie wydajności i niezawodności, wykrywanie i obsługę awarii: kontrolerów, dysków, baterii; wymianę dysków i baterii, aktualizację oprogramowania macierzy (jeśli akcje te muszą być wykonywana przez użytkownika);
c. macierzy obiektowej – tworzenie puli redundantnego przechowywania danych (Erasure Coding), konfigurację replikacji geograficznej, definiowanie przestrzeni, kont i kontenerów; monitoring macierzy obiektowej, wykrywanie i obsługę awarii: węzłów macierzy, kontrolerów dyskowych i ich baterii; wymianę dysków i innych elementów macierzy oraz aktualizację oprogramowania węzłów macierzy (jeśli akcje te muszą być wykonywana przez użytkownika);
d. sieci LAN – konfigurację przełączników, definiowanie adresacji i VLANów;
e. systemu UTM – definicji polityk ochrony sieci oraz obsługa zdarzeń/ wykrytych anomalii;
f. sieci SAN – definicja nazewnictwa i adresacji w sieci, konfigurowanie stref SAN:
g. systemu wykonywania kopii zapasowych – konfiguracja systemu; objaśnienie zdefiniowanych polityk wykonywania kopii zapasowych, pul przechowywania danych oraz sposobu monitorowania poprawności wykonywania kopii zapasowych a także procedur odtwarzania danych; demonstracja próbnego wykonania kopii zapasowej i odtwarzania dla minimum jednego z serwerów wirtualnych system wysokiej dostępności; monitoring systemu, wykrywanie awarii oraz czynności serwisowe, których wykonanie przez użytkownika zakłada się w zaoferowanym programie serwisowym;

6. Szkolenia:

b) Szkolenie z administracji oprogramowaniem z rodziny systemów operacyjnych Linux klasy enterprise dostarczonym z fizycznymi serwerami systemu wysokiej dostępności oraz systemu baz danych NoSQL
   a. Rodzaj szkolenia:
      i. autoryzowane,
      ii. przygotowujące uczestnika do zdania egzaminu na poziomie certyfikowanego administratora dostarczonego oprogramowania z rodziny systemów operacyjnych Linux klasy enterprise (CSA),
      iii. szkolenie musi zakończyć się egzaminem na poziomie certyfikowanego administratora dostarczonego oprogramowania z rodziny systemów operacyjnych linux klasy enterprise (CSA).
   b. Szkolenie i egzamin musi być przeznaczony dla 3 osób.

c) Szkolenie z administracji oprogramowania do wirtualizacji:
   a. Rodzaj szkolenia:
      i. autoryzowane lub
      ii. wykonane przez inżyniera Wykonawcy lub
      iii. wykonane przez producenta dostarczonego sprzętu lub oprogramowania.
   b. Szkolenie musi być co najmniej pięciodniowe.
   c. Szkolenie musi być z zakresu oprogramowania do wirtualizacji;
   d. Szkolenie musi obejmować tematykę z zakresu instalacji, konfiguracji oraz zarządzania oprogramowaniem do wirtualizacji;
   e. Szkolenie musi obejmować swoim zakresem co najmniej tematykę:
      i. wprowadzenia do software defined Data Center,
      ii. wpływ wirtualizatora na pamięć i procesory serwerów,
      iii. tworzenie, dostarczanie i usuwanie maszyn wirtualnych,
      iv. wyjaśnienie narzędzi związanych z wirtualizatorem,
      v. narzędzia zarządzania systemem wirtualizacji,
      vi. rozwiązywanie problemów związanych z systemami operacyjnymi serwerów i wirtualizatorem,
      vii. opis architektury systemu zarządzania wirtualizacją,
      viii. opis komunikacji hostów z systemem zarządzania,
      ix. identyfikacja usług systemu zarządzania,
      x. zasady kontroli dostępu,
      xi. monitorowanie, backup i odtworzenie systemu zarządzania wirtualizatorem,
      xii. konfiguracja i zarządzanie wirtualnymi sieciami,
      xiii. opis, zarządzanie i konfigurowanie wirtualnego switcha,
      xiv. opis rodzajów połączeń w ramach zwirtualizowanego przełącznika,
      xv. opis architektury stosu TCP/IP zwirtualizowanego przełącznika,
      xvi. komunikacja z sieciami VLAN fizycznych przełączników,
      xvii. konfiguracja i zarządzanie wirtualną pamięcią masową,
      xviii. identyfikacja protokołów zwirtualizowanej pamięci masowej,

xix. omówienie wykorzystania w wirtualnych hostach protokołów iSCSI, NFS i FC,
xx. konfiguracja, uruchomienie i zarządzanie wirtualnymi sieciami SAN
xxi. zarządzanie maszynami wirtualnymi (tworzenie VM, klony i szablony maszyn wirtualnych, tworzenie i zarządzania snapshotami maszyn wirtualnych),
xxii. monitoring i zarządzanie zasobami zwirtualizowanymi (konfiguracja i zarządzanie zasobami, rozwiązywanie problemów związanych z nadmiernym obciążaniem zasobów, wykorzystanie technologii optymalizacji wykorzystania zasobów),
xxiii. tworzenie klastrów HA.

f. Po ukończeniu szkolenia, każdy uczestnik otrzyma stosowny dokument potwierdzający uzyskanie kompetencji do administrowania dostarczonym oprogramowaniem do wirtualizacji i pozwalający na przystąpienie do egzaminu certyfikującego na poziomie co najmniej podstawowym z zakresu instalacji, konfiguracji i zarządzania systemem do wirtualizacji
g. Po ukończeniu szkolenia uczestnik ma otrzymać voucher pozwalający na przystąpienie do egzaminu certyfikującego na poziomie co najmniej podstawowym z zakresu instalacji, konfiguracji oraz zarządzania oprogramowaniem do wirtualizacji.
h. Szkolenie będzie się odbywało na terenie Katowic lub wykonawca pokryje koszty transportu i noclegu w przypadku miejsca szkolenia innego niż Katowice.
i. Szkolenie przeznaczone dla trzech osób

d) Szkolenie z administracji macierzą dyskową:
   a. Rodzaj szkolenia:
      i. autoryzowane lub
      ii. wykonane przez inżyniera Wykonawcy lub
      iii. wykonane przez producenta dostarczonego sprzętu lub oprogramowania.
   b. Szkolenie musi być co najmniej trzydniowe.
   c. Szkolenie musi być z zakresu zarządzania macierzą dyskową.
   d. Szkolenie musi być przeprowadzone w postaci warsztatów co najmniej w zakresie:
      i. teorii dotyczącej zasad funkcjonowania sieci SAN
      ii. konfiguracji oraz obsługi macierzy blokowej
      iii. omówienia budowy i zasady działania urządzenia
      iv. tworzenia zasobów logicznych
      v. konfiguracji funkcjonalności LUN masking
      vi. prezentacji zasobów do systemów operacyjnych
      vii. migracji zasobów logicznych
      viii. diagnozy pracy urządzenia
      ix. omówienia budowy urządzenia
         1. tworzenia systemów plików
         2. praw dostępu do plików, quota
         3. rodzajów i zasad konfiguracji
         4. protokołów dostępu do danych plikowych
         5. prezentacji zasobów serwerom
         6. diagnozy pracy urządzenia
      x. Po ukończeniu szkolenia, każdy uczestnik otrzyma dokument potwierdzający uzyskanie kompetencji do administrowania dostarczoną macierzą dyskową.
      xi. Szkolenie będzie się odbywało na terenie Katowic lub wykonawca pokryje koszty transportu i noclegu w przypadku miejsca szkolenia innego niż Katowice.
      xii. Szkolenie przeznaczone dla trzech osób.

e) Szkolenie z administracji obiektowym systemem składowania danych:
   a. Rodzaj szkolenia:
      i. autoryzowane lub
      ii. wykonane przez inżyniera Wykonawcy lub
      iii. wykonane przez producenta dostarczonego sprzętu lub oprogramowania.
   b. Szkolenie musi być co najmniej trzydniowe.
   c. Szkolenie musi być z zakresu zarządzania obiektowym systemem składowania danych. Szkolenie musi być przeprowadzone w postaci warsztatów,
   d. Po ukończeniu szkolenia, każdy uczestnik ma otrzymać stosowny dokument potwierdzający uzyskanie kompetencji do administrowania dostarczoną macierzą dyskową,
   e. Szkolenie będzie się odbywało na terenie Katowic lub wykonawca pokryje koszty transportu i noclegu w przypadku miejsca szkolenia innego niż Katowice,
   f. Szkolenie przeznaczone dla trzech osób

f) Szkolenie z zakresu sieci:

a. Szkolenie z administracji przełącznikami LAN i FC
   i. Rodzaj szkolenia:
      1. autoryzowane lub
      2. wykonane przez inżyniera Wykonawcy lub
      3. wykonane przez producenta dostarczonego sprzętu lub oprogramowania.
   ii. Szkolenie musi być co najmniej jednodniowe,
   iii. Szkolenie musi być z zakresu dostarczonych przełączników LAN oraz SAN. Szkolenie musi obejmować pełen zakres informacji na temat zarządzania dostarczonym przełącznikiem sieciowym i światłowodowym,
   iv. Po ukończeniu szkolenia, każdy uczestnik ma otrzymać stosowny dokument potwierdzający uzyskanie kompetencji do administrowania dostarczonym przełącznikiem sieciowym i światłowodowym,
   v. Szkolenie będzie się odbywało na terenie Katowic lub wykonawca pokryje koszty transportu i noclegu w przypadku miejsca szkolenia innego niż Katowice.
   vi. Szkolenie przeznaczone dla trzech osób.

b. Szkolenie z administracji klastrem zapór sieciowych:
   i. Rodzaj szkolenia:
      1. autoryzowane lub
      2. wykonane przez inżyniera Wykonawcy lub
      3. wykonane przez producenta dostarczonego sprzętu lub oprogramowania.
   ii. Szkolenie musi być co najmniej pięciodniowe,
   iii. Szkolenie musi być z zakresu dostarczonego klastra zapór sieciowych jego administracji i konfiguracji w tym m.in.:
      1. budowa klastra zapór sieciowych,
      2. omówienie funkcjonalności jaka jest dostępna dla klastra zapór sieciowych;
      3. omówienie zasad budowania zapór i konfigurowania zapór w oparciu o klaster zapór sieciowych.
   iv. Po ukończeniu szkolenia, każdy uczestnik ma otrzymać dokument potwierdzający uzyskanie kompetencji do administrowania dostarczonym klastrem zapór sieciowych.
   v. Szkolenie będzie się odbywało na terenie Katowic lub wykonawca pokryje koszty transportu i noclegu w przypadku miejsca szkolenia innego niż Katowice.
   vi. Szkolenie przeznaczone dla trzech osób.

g) Szkolenie administracji: backup
   a. Rodzaj szkolenia:
      i. autoryzowane lub
      ii. wykonane przez inżyniera Wykonawcy lub
      iii. wykonane przez producenta dostarczonego sprzętu lub oprogramowania.
   b. Szkolenie musi być co najmniej czterodniowe dniowe.
      i. Szkolenie musi obejmować pełen zakres możliwości oprogramowania do wykonywania kopii zapasowych
      ii. Szkolenie musi być co najmniej 1 dniowe z zakresu obsługi serwera.
   c. Po ukończeniu szkolenia, każdy uczestnik ma otrzymać stosowny dokument potwierdzający uzyskanie kompetencji do administrowania dostarczonym systemem backupu.
   d. Szkolenie będzie się odbywało na terenie Katowic lub wykonawca pokryje koszty transportu i noclegu w przypadku miejsca szkolenia innego niż Katowice.
   e. Szkolenie przeznaczone dla trzech osób.

7. Instalacja okablowania światłowodowego w Centrum Zapasowym:

a) W ramach instalacji elementów infrastruktury serwerowej dostarczonej w ramach realizacji zamówienia do Centrum Zapasowego Biblioteki Śląskiej Wykonawca musi zainstalować połączenie światłowodowe w budynku Biblioteki Śląskiej przy ul. Ligonia 7 w Katowicach łączące serwerownię w piwnicy budynku z obecnym miejscem zakończenia światłowodu w serwerowni na I piętrze budynku.

b) Instalacja połączenia obejmuje zaprojektowanie trasy, ułożenie i instalację światłowodu oraz pomiary kontrolne jakości połączenia i przekazanie dokumentacji połączenia Zamawiającemu. Połączenie należy wykonać pomiędzy Centrum Zapasowym (w piwnicy Biblioteki Śląskiej na ul. Ligonia 7) a obecnym miejscem zakończenia światłowodu (pomieszczenie Biblioteki Śląskiej na ul. Ligonia 7, serwerownia I piętro). Połączenie musi być wykonane wraz z przyłączami i wszystkimi niezbędnymi elementami umożliwiającymi podłączenie infrastruktury serwerowej zainstalowanej w szafie w Centrum Zapasowym do infrastruktury LAN Biblioteki Śląskiej na ul. Ligonia 7 (zlokalizowanej na I piętrze). Orientacyjna długość połączenia (trasy światłowodowej) to około 20 m..

OPIS MIEJSCA INSTALACJI ORAZ DROGI DOSTAWY:

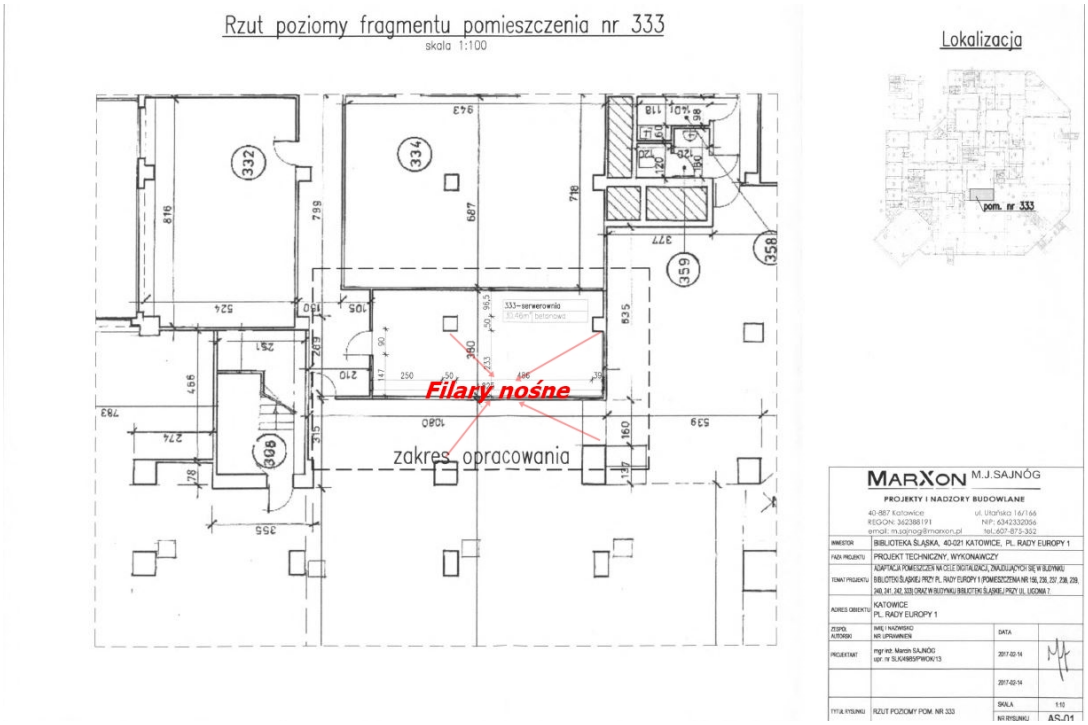
Infrastruktura serwerowa będąca przedmiotem zamówienia będzie zainstalowana w dwóch centrach danych w pomieszczeniach serwerowni Biblioteki Śląskiej:

1. Centrum Podstawowym (CP) – w budynku Biblioteki Śląskiej na Placu Rady Europy 1 w Katowicach.
2. Centrum Zapasowym (CZ) – w budynku Biblioteki Śląskiej przy ul. Ligonia 7 w Katowicach.

Ponadto elementy sieci LAN dla pracowni digitalizacyjnych i czytelni Biblioteki Śląskiej zostaną zainstalowane w pomieszczeniach tych pracowni znajdujących się przy Placu Rady Europy 1 w Katowicach, w tzw. Lokalnych Punktach Dystrybucyjnych (szafy podwieszone w pomieszczeniach pracowni i holu głównym BŚ).

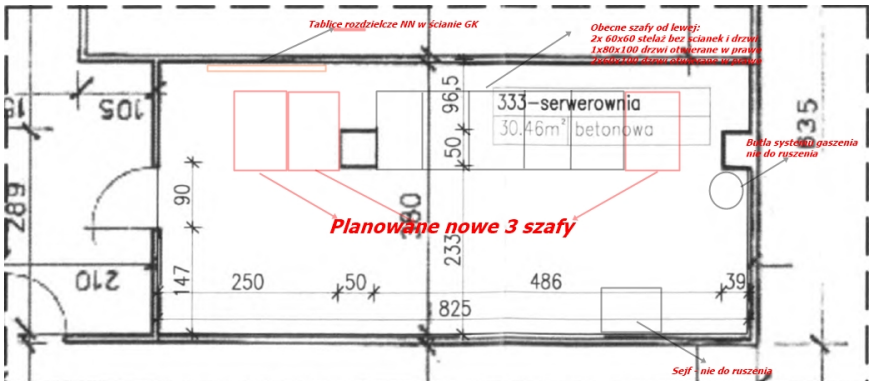
1. Centrum Podstawowe (CP):

Pomieszczenie serwerowni: w Centrum Podstawowym zakłada się umieszczenie elementów dostarczanej infrastruktury serwerowej w pomieszczeniu serwerowni zlokalizowanym na 2. piętrze budynku. Schemat (rzut) pomieszczenia serwerowni oraz jego umiejscowienie na kondygnacji zawiera poniższy Rysunek 1.

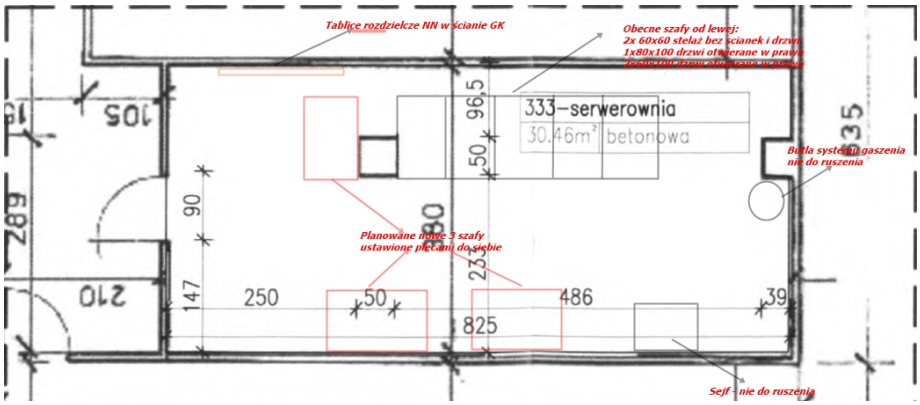


Rysunek 1 Schemat pomieszczenia serwerowni Centrum Podstawowego

Możliwe warianty rozmieszczenia szaf w Centrum Podstawowym na potrzeby instalacji dostarczanej infrastruktury serwerowej przedstawiają poniższe rysunki: Rysunek 2 i Rysunek 3.



Rysunek 2. Możliwe warianty umieszczenia szaf przemysłowych w Centrum Podstawowym (wariant 1)



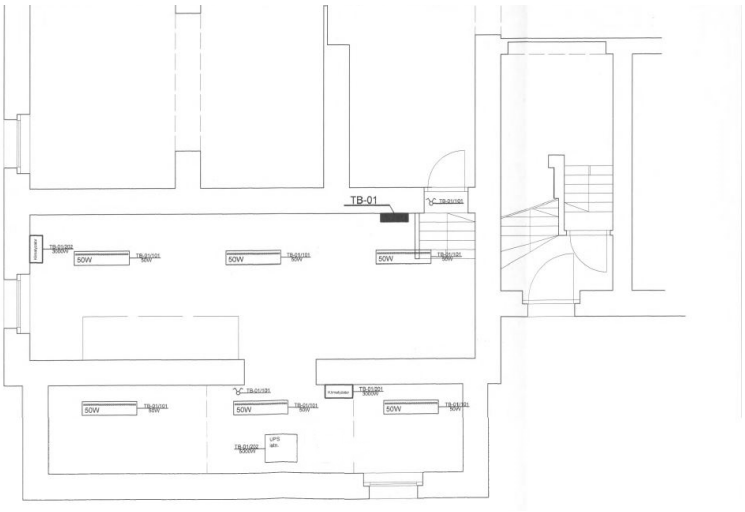
Rysunek 3. Możliwe warianty umieszczenia szaf przemysłowych w Centrum Podstawowym (wariant 2)

Ograniczenia dotyczące rozmiarów i rozmieszczenia szaf. W Centrum Podstawowym, w obu wariantach umiejscowienia szaf, dla szaf zainstalowanych w istniejącym rzędzie szaf na „górze" pomieszczenia (wg rysunku) należy zaprojektować szafy o szerokości zewnętrznej maksimum 80cm i głębokości zewnętrznej maksimum **100 cm**, ze względu na konieczność zachowania odstępu od tablic rozdzielczych NN (oznaczonych na rysunkach) na „górnej" ścianie pomieszczenia (wg rysunku). Należy założyć, że fronty dostarczanych szaf zostaną zrównane z szafami istniejącymi. Szafy wraz z drzwiami tylnymi muszą zapewniać dostęp do zainstalowanego w nich sprzętu w taki sposób, by możliwe było przeprowadzenie podstawowych czynności serwisowych (podłączenie/ kontrola stanu okablowania, wymiana zasilaczy, wymiana napędów dyskowych – jeśli są one dostępne od tyłu serwerów/macierzy). Z tyłu szafy należy zastosować drzwi dzielone, 2-skrzydłowe. Z przodu szaf należy zastosować drzwi „prawe" lub drzwi 2-skrzydłowe.
Ponadto, w wariancie 2. należy zaprojektować szafy zaplanowane do ustawienia przy „dolnej" ścianie pomieszczenia (wg rysunku) o szerokości zewnętrznej maksimum 80cm oraz takiej głębokości zewnętrznej (ale nie większej niż **100 cm**), by możliwe było ich ustawienie w taki sposób, iż szafy te będą ustawione „plecami do siebie", z zachowaniem dystansu między tymi szafami pozwalającego na prowadzenie podstawowych czynności serwisowych (podłączenie/ kontrola stanu okablowania, wymiana zasilaczy, wymiana napędów dyskowych – jeśli elementy te dostępne są od tyłu serwerów/macierzy) a jednocześnie możliwe będzie pełne otwarcie drzwi frontowych szaf, w celu prowadzenia instalacji sprzętu oraz podstawowych czynności serwisowych (podłączenie/ kontrola stanu okablowania, wymiana napędów dyskowych – jeśli są one dostępne od frontu i/lub góry serwerów) oraz pełne (w zakresie ruchu prowadnic oraz w celu wymiany serwerów i prowadnic) wysunięcie elementów infrastruktury – serwerów czy półek dyskowych macierzy. Z tyłu tych szaf należy zastosować drzwi dzielone, 2-skrzydłowe, z przodu drzwi o orientacji pozwalającej na pełny dostęp do wnętrza szafy lub drzwi dzielone, 2-skrzydłowe.

Droga dostawy: W Centrum Podstawowym dostawa sprzętu do serwerowni zlokalizowanej na 2 piętrze budynku możliwa jest poprzez wejście tylne do budynku od strony parkingu wewnętrznego po północno-wschodniej stronie budynku. Wjazd na parking od ulicy Granicznej (w prawo za stacją Shell w prawo, jadąc z kierunku północnego). W budynku dostawa powinna odbywać się poprzez ciąg komunikacyjny obejmujący: drzwi wejściowe o prześwicie 180x190cm (szerokość x wysokość), następnie korytarz, na którym w środku długości korytarza znajdują się drzwi o prześwicie 140x200cm, kolejno drzwi wejściowe do klatki schodowo/windowej o prześwicie 90x190cm. W tym miejscu możliwe jest skorzystanie z windy osobowej o nośności maksymalnej 630 kg – drzwi windy o prześwicie 80x190cm. Alternatywnie (jeśli nie korzysta się z windy) droga przez klatkę schodową: drzwi klatki schodowej o prześwicie 90x190cm, dwa piętra schodami, następnie drzwi klatki schodowej o prześwicie 90x190cm. Od tego miejsca droga jest tożsama z wyjściem z windy - kolejno drzwi klatki schodowo/windowej 90x190cm, następnie korytarzem do serwerowni, drzwi serwerowni o prześwicie: 90x200cm.

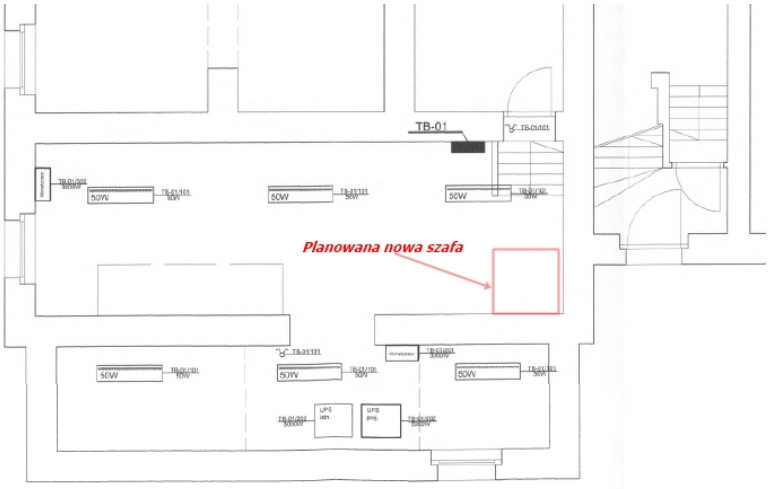
2. Centrum Zapasowe (CZ):

Pomieszczenie serwerowni: w Centrum Zapasowym zakłada się umieszczenie elementów dostarczanej infrastruktury serwerowej w pomieszczeniu serwerowni zlokalizowanym w piwnicy budynku. Schemat (rzut) pomieszczenia oraz jego umiejscowienie na kondygnacji zawiera poniższy Rysunek 4.

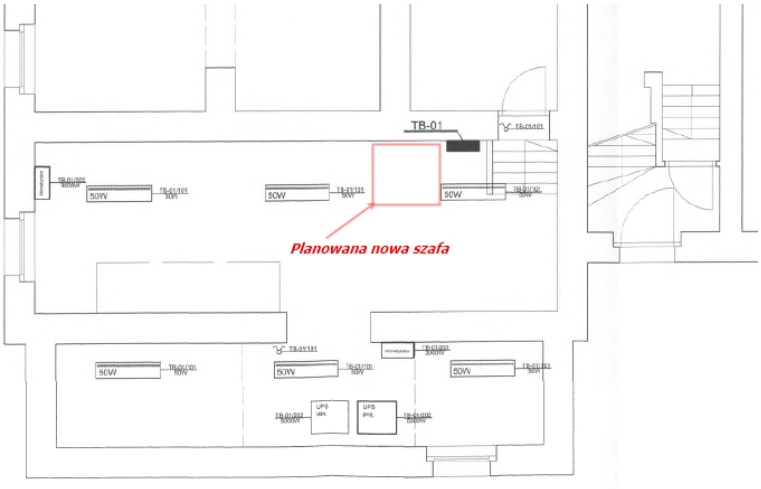


Rysunek 4 Schemat pomieszczenia serwerowni Centrum Zapasowego

Możliwe warianty rozmieszczenia szaf w Centrum Podstawowym na potrzeby instalacji dostarczanej infrastruktury serwerowej przedstawiają poniższe rysunki: Rysunek 5 i Rysunek 6.



Rysunek 5 Schemat rozmieszczenia szaf w serwerowni Centrum Zapasowego (wariant 1)



Rysunek 6 Schemat rozmieszczenia szaf w serwerowni Centrum Zapasowego (wariant 2)

Ograniczenia dotyczące rozmiarów i rozmieszczenia szaf. W Centrum Zapasowym przewiduje się instalację jednej szafy przemysłowej. W obu wariantach umiejscowienia szafy (przy ścianie „górnej" lub przy ścianie „dolnej" wg rysunku), należy zaprojektować szafę o szerokości zewnętrznej maksimum 80cm i głębokości zewnętrznej maksimum **100 cm**, ze względu na konieczność zachowania odstępu szafy od ścian oraz zachowanie przejścia przez pomieszczenie. Szafa wraz z drzwiami musi zapewniać dostęp do zainstalowanego w nich sprzętu w taki sposób, by możliwe było przeprowadzenie podstawowych czynności serwisowych (podłączenie/ kontrola stanu okablowania, wymiana zasilaczy, wymiana napędów dyskowych – od tyłu szafy - jeśli te elementy są dostępne od tyłu serwerów/macierzy. Ponadto trzeba zapewnić możliwość pełnego otwarcia drzwi frontowych szafy, w celu prowadzenia instalacji sprzętu oraz podstawowych czynności serwisowych (podłączenie/ kontrola stanu okablowania, wymiana napędów dyskowych – jeśli są one dostępne od frontu i/lub góry serwerów) oraz pełne (w zakresie ruchu prowadnic oraz w celu wymiany serwerów i prowadnic) wysunięcie elementów infrastruktury – serwerów czy półek dyskowych macierzy. Z tyłu szafy należy zastosować drzwi dzielone, 2-skrzydłowe, z przodu drzwi o orientacji pozwalającej na pełny dostęp do wnętrza szafy lub drzwi dzielone, 2-skrzydłowe.

Droga dostawy: W Centrum Zapasowym dostawa sprzętu do serwerowni zlokalizowanej w piwnicy budynku przy ul. Ligonia 7 możliwa jest poprzez wejście tylne do budynku od strony podwórza zlokalizowane w środkowej części budynku (południowa ściana budynku), wjazd na parking od ulicy Ligonia, poprzez bramę wjazdową zlokalizowaną pomiędzy numerami Ligonia 1 i 3. W budynku dostawa musi odbywać się poprzez ciąg komunikacyjny obejmujący: Drzwi wejściowe (uwaga! prześwit 80x180cm!), bezpośrednio za drzwiami dwa różnej wysokości stopnie, pierwszy o wysokości 25cm, drugi 15cm, następnie przejście na korytarz przez drzwi 90x195cm za drzwiami korytarz z najniższym punktem 195cm oraz najwęższym prześwitem poziomym 150cm, następnie drzwi do pomieszczenia, w którym będzie stała szafa – prześwit drzwi: 90x195cm, za drzwiami schody, 5 stopni. Nie jest możliwe skorzystanie z windy osobowej/towarowej.

III. SPECYFIKACJA TECHNICZNA ELEMENTÓW INSTRASTRUKTURY SERWEROWEJ

W kolejnych punktach specyfikacji technicznej omówiono architekturę oraz cechy jakościowe i funkcjonalności dla poszczególnych elementów infrastruktury serwerowej.
Wszystkie elementy dostarczanej infrastruktury serwerowej muszą być fabrycznie nowe i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy. Zaoferowany przedmiot zamówienia na dzień złożenia oferty nie może być przeznaczony przez producenta do wycofania z produkcji, sprzedaży, licencjonowania lub wsparcia – nie może mieć statusu ang. „End of Life".
Dostarczane 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 i własnościowych praw autorskich osób trzecich.

1. SERWERY SYSTEMU WYSOKIEJ DOSTĘPNOŚCI I SERWER BAZ DANYCH NOSQL

System wysokiej dostępności obejmuje 12 serwerów fizycznych wraz z platformą wirtualizacyjną oraz co najmniej 24 serwerami wirtualnymi. W systemie wysokiej dostępności należy uruchomić co najmniej 20 maszyn wirtualnych z systemami operacyjnymi z rodziny Linux oraz minimum 4 instancje Windows Server 2019.

Poniżej opisane są wymagania dla serwerów fizycznych dla systemu wysokiej dostępności oraz dla platformy wirtualizacyjnej systemu wysokiej dostępności oraz systemów operacyjnych maszyn wirtualnych.

A.I. Serwer fizyczny systemu wysokiej dostępności

Serwer fizyczny systemu wysokiej dostępności musi spełniać co najmniej poniższe wymagania – przy czym wszystkie określone wymagania muszą być traktowane jako minimalne, chyba że treść wymogu stanowi inaczej:

1. **Procesory:**
    1. dwa procesory ogólnego przeznaczenia, w architekturze x86_64, które mają możliwość wykonywania 64-bitowego kodu (np. EMT64T);
    2. obydwa procesory muszą być identyczne, tego samego typu, wykonane w tej samej technologii, posiadać taką samą liczbę rdzeni oraz być taktowane zegarem o takiej samej prędkości;
    3. minimalna sumaryczna liczba rdzeni fizycznych procesorów w serwerze: 32;
    4. procesory muszą wspierać funkcjonalność procesorów logicznych (np. *hyper threading*);
    5. minimalna prędkość taktowania procesorów [GHz]: 2.1
    6. maksymalne całkowite ogólne zużycie energii zainstalowanych procesorów [W]: 250
2. **Pamięć operacyjna:**
    1. Minimalna pojemność zainstalowanej pamięci per serwer to **256 GB**
    2. Liczba kości pamięci musi zapewniać maksymalną przepustowość, tj. pełną obsadę kanałów pamięci;
    3. Dopuszczalne jest zainstalowanie co najwyżej 1 kości pamięci na kanał kontrolera pamięci
    4. Wszystkie moduły pamięci w ramach muszą być identyczne, tego samego typu, wykonane w tej samej technologii i o tej samej pojemności oraz muszą charakteryzować się takimi samymi parametrami pracy
    5. Wszystkie moduły pamięci muszą pracować z najwyższą wspieraną przez procesor częstotliwością;
    6. Wszystkie dostarczone moduły pamięci muszą być wyposażone w mechanizm korekcji błędów ECC
    7. Wielkość obsługiwanej przez serwer pamięci – minimum 1024GB
3. **Pamięć masowa – podsystem dyskowy** – serwera musi umożliwiać uruchamianie oraz utrzymanie a także zabezpieczanie danych środowiska produkcyjnego w sposób wydajny i niezawodny; wydajność podsystemu dyskowego jest określona zdefiniowanymi poniżej minimalnym wymaganiami dla dysków magnetycznych HDD i napędów pamięci SSD/NVMe; niezawodność musi być zapewniona m.in. poprzez zwielokrotnienie komponentów sprzętowych obejmujące dyski magnetyczne oraz SSD/NVMe oraz zastosowanie dla nich mechanizmów redundantnego przechowywania danych (RAID) a także zabezpieczenie zawartości cache do zapisu przed utratą w przypadku awarii zasilania; parametry minimalne elementów podsystemu dyskowego:
    1. *Zatoki na dyski magnetyczne/talerzowe/rotacyjne (HDD) – nie dotyczy*;
    2. Zatoki/sloty na napędy/moduły pamięci SSD/NVMe - dla danych platformy wirtualizacyjnej:
        1. Minimalna liczba zatok 2,5" lub slotów PCIe lub M.2 dla pamięci SSD/NVMe: **8**
        2. Minimalna liczba zainstalowanych napędów/modułów pamięci SSD/NVMe: 2
        3. Wsparcie *hot-swap* dla zatok/slotów na napędy/moduły pamięci SSD/NVMe: tak
    3. Napędy/moduły pamięci SSD/NVMe - dla danych platformy wirtualizacyjnej:
        1. Minimalna katalogowa pojemność [GB]: 1600
        2. Minimalna wydajność zapisu losowego (blok 4kB) [IOPS]: 80 000
        3. Minimalna wydajność odczytu losowego (blok 4kB) [IOPS]: 150 000

4. Minimalna wydajność zapisu sekwencyjnego (blok 1MB) [MB/s]: 1000
5. Minimalna wydajność odczytu sekwencyjnego (blok 1MB) [MB/s]: 2000
6. Maksymalne opóźnienie (zapis) [mikro-sekundy]: 20
7. Minimalny MTBF (ang. *Mean Time Between Failures*) [godzin]: 2 000 000
8. Minimalna odporność na ścieranie [DWPD (ang. *disk writes per day*)]: 3
9. Interfejsy napędów/modułów pamięci SSD/NVMe: SATA 3.0 6GBit/s lub SAS lub PCIe lub M.2
10. Technologia pamięci: NAND, np. V-NAND lub 3D NAND TLC

4. Dyski magnetyczne (HDD) – nie dotyczy;

5. Kontrolery dyskowe / kontrolery pamięci SSD/NVMe
   1. Liczba portów kontrolerów napędów / modułów pamięci SSD/NVME musi być wystarczająca do podłączenia wszystkich wymaganych napędów / modułów pamięci SSD/NVME;
   2. Typy RAID wspierane przez kontrolery
      1. Dla napędów/modułów SSD/NVMe – dla danych platformy wirtualizacyjnej – minimum RAID1 oraz RAID10
      2. *Dla dysków magnetycznych (HDD) – nie dotyczy;*
   3. Niezawodność:
      1. Cache do zapisu kontrolera RAID musi być zabezpieczona przed utratą zawartości w przypadku awarii zasilania;
      2. Mechanizm zabezpieczenia pamięci cache może wykorzystywać baterię lub kondensator podtrzymującą zasilanie pamięci cache lub inne rozwiązanie o analogicznej funkcjonalności;
      3. Zastosowanie zewnętrznego zasilacza UPS jest traktowane jako zabezpieczenie zawartości cache do zapisu kontrolera RAID; takie zabezpieczenie kontrolera RAID musi być zapewnione niezależnie od faktu zastosowania w projektowanym rozwiązaniu zasilacza awaryjnego UPS;

4. **Interfejsy sieciowe –** muszą zapewniać możliwość realizacji niezawodnych połączeń systemu wysokiej niezawodności do sieci LAN/WAN oraz wydajność dostępu do usług i aplikacji działających na serwerach systemu wysokiej niezawodności oraz dostępu do danych składowanych w serwerach; niezawodność musi zostać zrealizowana poprzez redundancję portów po stronie serwera; wydajność połączeń sieciowych musi zostać zapewniona przez zaoferowanie odpowiedniej sumarycznej przepustowości interfejsów sieciowych; minimalne parametry i funkcjonalność interfejsów sieciowych:
   1. wymagane interfejsy sieciowe:
      1. interfejsy do *zarządzania*:
         1. min. 1 interfejs Ethernet 1Gbit lub szybszy na potrzeby dostępu do konsoli systemu operacyjnego (zdalny pulpit, SSH, dostęp do konsoli platformy wirtualizacyjnej);
         2. min. 1 interfejs Ethernet 1Gbit dedykowany do zarządzania (IPMI);
      2. interfejsy sieci LAN *produkcyjnej:*
         1. min. 2 interfejsy 10 Gbit Ethernet lub szybsze do sieci *LAN (a poprzez LAN do sieci WAN);*
         2. min. 2 interfejsy 10 Gbit Ethernet lub szybsze dedykowane dla połączenia serwerów z systemem wykonywania kopii zapasowych (za pośrednictwem przełączników LAN)*;*
         3. interfejsy sieci produkcyjnej muszą wspierać możliwość łączenia w strukturę działającą w trybie wysokiej niezawodności (min. tryb *active-passive*, bez wykorzystania LACP);
      3. interfejsy sieci *SAN/FC:*
         1. min. 2 interfejsy 16 Gbit FC lub szybsze do sieci *SAN/FC;*
         2. interfejsy sieci SAN muszą wspierać możliwość działania w trybie dostępu wielościeżkowego serwerów do wolumenów w macierzy dyskowej (centralnej) dostarczanej przez Wykonawcę;
   2. Interfejsy sieciowe LAN serwera zostaną podłączone do dostarczanych przez Wykonawcę przełączników sieci LAN, Wykonawca jest zobowiązany do dostarczeni dla serwerów odpowiednich wkładek oraz okablowania do podłączenia serwerów do sieci LAN;
   3. Interfejsy sieciowe SAN serwera zostaną podłączone do dostarczanych przez Wykonawcę przełączników sieci SAN, Wykonawca jest zobowiązany do dostarczeni dla serwerów odpowiednich wkładek oraz okablowania do podłączenia serwerów do sieci SAN;
   4. interfejsy sieciowe LAN i SAN muszą znajdować się na liście zgodności sprzętowej zaoferowanych serwerów; muszą być także kompatybilne z platformami wirtualizacyjnymi VMware vSphere 7, RedHat Virtualization 4 oraz systemami operacyjnymi RedHat Enterprise Linux 8, Suse Enterpise Linux Server 15 i Windows Server 2019, tzn. muszą się znajdować na liście kompatybilności tych systemów lub specyfikacja interfejsów sieciowych dostępna na witrynach producenta lub załączona do oferty musi wskazywać kompatybilność interfejsów sieciowych z tymi systemami operacyjnymi.

5. **Zarządzanie serwerem**:
   1. serwer musi wspierać zarządzanie zgodne z protokołem IPMI w wersji min. 2.0 (lub KVM-over-LAN)
   2. serwer musi posiadać diody sygnalizacyjne dla zasilania i aktywności sieci oraz aktywności dysków;

6. **Karta graficzna:**

1. Zintegrowana, pozwalająca na wyświetlanie konsoli graficznej systemu operacyjnego z rozdzielnością 1920x1200 oraz współpracę z zaoferowaną konsolą oraz przełącznikiem/hubem dla serwerów;

7. **Zasilanie:**
   1. Minimum podwójne zasilacze co najmniej klasy 80 PLUS Platinum w konfiguracji redundantnej;
   2. moc zasilaczy musi być wystarczająca do zasilenia serwera przy całorocznej pracy ciągłej i pełnym wykorzystaniu wszystkich komponentów serwera;
   3. musi być możliwość wymiany zasilaczy w trybie *hot-plug;*
   4. zasilacze muszą być zabezpieczone przed przypadkowym wysunięciem podczas wykonywania czynności obsługowych / serwisowych;
8. **Obudowa, okablowanie, instalacja:**
   1. Serwer nie może być wyższy niż **1U** oraz musi być dopasowany do szafy przemysłowej 19";
   2. Serwer musi być wyposażony w szyny montażowe umożliwiające wysunięcie serwera umożliwiające wykonanie czynności serwisowych (w tym wymiana dysków / modułów pamięci SSD/NVMe) bez konieczności wyłączania serwera – nawet w przypadku, gdy serwer ten zostanie zamontowany w szafie serwerowej w bezpośrednim sąsiedztwie innych urządzeń takich jak inne rackowalne serwery czy przełączniki sieci LAN/SAN
   3. Serwer musi być wyposażony w prowadnice i pantografy dla okablowania; muszą one zapewniać ochronę okablowania serwera przed uszkodzeniem podczas wymiany dysków HDD i modułów pamięci SSD/NVMe i/lub zasilaczy oraz innych modułów wymienialnych przez użytkownika / serwis;
   4. Okablowanie serwera musi być poprowadzone zgodnie z dobrymi praktykami – w tym m.in. z zachowaniem minimalnych promieni gięcia dla okablowania światłowodowego (jeśli jest stosowane);
9. **Certyfikacja/zgodność:**
   1. Zgodność z RoHS
   2. Zgodność z deklaracją CE
   3. Serwer musi być obecny na liście kompatybilności systemów: VMware vSphere 7, RedHat Virtualization oraz RedHat Enterprise Linux 8, Suse Enterpise Linux Server 15 i Windows Server 2019.

A.II. Platforma wirtualizacyjna oraz systemy operacyjne serwerów systemu wysokiej dostępności

1. Platforma wirtualizacyjna dla serwerów systemu wysokiej dostępności

Platforma wirtualizacyjna oraz systemy operacyjne uruchamiane na serwerach systemu wysokiej dostępności muszą spełniać co najmniej poniższe wymagania (przy czym wszystkie określone wymagania muszą być traktowane jako minimalne, chyba że treść wymogu w sposób jednoznaczny stanowi inaczej):

1) Wraz z serwerami systemu wysokiej dostępności opisanymi w punkcie A.I SIWZ musi zostać dostarczone oprogramowanie systemów operacyjnych i platforma wirtualizacyjna;
2) Oprogramowanie do wirtualizacji musi mieć architekturę i model licencyjny umożliwiające uruchomienie minimum 24 maszyn wirtualnych na 12 serwerach fizycznych systemu wysokiej dostępności.
3) *Zapewnienie **możliwości uruchomienia dodatkowo 24 maszyn wirtualnych** w systemie wysokiej dostępności jest funkcjonalnością **dodatkowo punktowaną** – patrz opis kryterium technicznego V.*
4) W ramach wymaganych 24 maszyn wirtualnych możliwych do uruchomienia w systemie wysokiej dostępności musi być możliwe uruchomienie:
   a. co najmniej 20 maszyn wirtualnych z systemami operacyjnymi z rodziny Linux
   b. minimum 4 instancji systemu Windows Server 2019
5) Oprogramowanie do wirtualizacji musi być kompatybilne z systemem do wykonywania kopii zapasowych opisanym w punkcie 5 SIWZ., tzn. musi być możliwe – za pomocą tego oprogramowania do wykonywania kopii zapasowych – zabezpieczanie środowiska wirtualnego działającego na systemie wysokiej dostępności poprzez wykonywanie kopii bezpieczeństwa danych (wolumenów dyskowych) maszyn wirtualnych składowanych na macierzy centralnej i/lub na dyskach wewnętrznych serwerów oraz kopii danych konfiguracyjnych środowiska do wirtualizacji oraz odtwarzanie tych danych w przypadku awarii;
6) Oprogramowanie do wirtualizacji musi posiadać następujące minimalne funkcje:
   1) Wsparcie co najmniej dla następujących systemów operacyjnych maszyn wirtualnych: RedHat Enterprise Linux 8, Suse Enterpise Linux Server 15 oraz Windows 10 i Windows Server 2019.
   2) Centralna konsola graficzną do zarządzania wieloma maszynami wirtualnymi oraz ich zasobami pracującymi na serwerze fizycznym, w tym:
      a. widok całego systemu i zbioru maszyn wirtualnych;
      b. widok zasobów dyskowych: puli dyskowych i skonfigurowanych na nich maszyn wirtualnych;
      c. widok wirtualnych sieci oraz powiązanych z nimi (używających ich) maszyn wirtualnych;
      d. możliwość monitorowania maszyn wirtualnych w zakresie co najmniej: stan maszyny wirtualnej (włączona/wyłączona), zużycie zasobów CPU, RAM i dyskowych oraz sieciowych;

3) Tekstowa konsola graficzna oraz publicznie udokumentowane API do zarządzania platformą wirtualizacyjną oraz maszynami wirtualnymi oraz zasobami fizycznymi i wirtualnym serwerów;
4) Wirtualizacja i zarządzanie zasobami dla maszyn wirtualnych::
    a. zasoby CPU i RAM:
        i. Obsługa do 12TB pamięci RAM per serwer fizyczny
        ii. Obsługa do 64 serwerów per klaster wirtualizacyjny.
        iii. Wsparcie do 128 wirtualnych CPU (vCPU) oraz 4TB RAM per serwer wirtualny
        iv. Możliwość dodawania pamięci RAM do maszyn wirtualnych na gorąco;
        v. Wsparcie dla tzw. ang. *overcommitment* RAM; w szczególności wsparcie dla tzw. balonowania pamięci operacyjnej maszyn wirtualnych (ang. *memory balooning*)
        vi. Możliwość dodawania vCPU i pamięci RAM do maszyn wirtualnych na gorąco;
    b. zasoby sieciowe:
        i. wsparcie dla VLAN, tagowania ramek, QoS oraz Jumbo Frames
        ii. możliwość zarządzania portami maszyn wirtualnych oraz wirtualnymi sieciami, w tym tzw. wirtualnymi przełącznikami
        iii. wsparcie dla tzw. *bonding* interfejsów sieciowych
        iv. Możliwość dodawania interfejsów sieciowych do maszyn wirtualnych na gorąco
    c. Wspierane tryby pracy maszyn wirtualnych:
        i. Możliwość działania maszyn wirtualnych w trybie wysokiej niezawodności (HA)
        ii. Możliwość przenoszenia w locie maszyn wirtualnych pomiędzy serwerami fizycznymi środowiska wirtualnego (bez zatrzymywania maszyn wirtualnych)
    d. wolumeny dyskowe:
        i. tworzenie obrazów maszyn wirtualnych; klonowanie maszyn wraz ze wsparciem dla rekonfiguracji klonowanych obrazów w locie (przed sklonowaniem i uruchomieniem)
        ii. wykonywanie wielu kopii migawkowych (ang. *snapshot*) w każdym momencie pracy maszyny wirtualnej oraz możliwość powrotu do jej stanu z każdego momentu wykonania kopii migawkowej;
        iii. możliwość przenoszenia w locie maszyn wirtualnych pomiędzy rozłącznymi pulami dyskowymi (bez zatrzymywania maszyn wirtualnych);
    e. sieciowe zasoby przechowywania danych:
        i. wsparcie możliwości tworzenia wolumenów dla maszyn wirtualnych na bazie przestrzeni dyskowej udostępnianej protokołami SMB oraz NFS (V3 i V) oraz na bazie przestrzeni dyskowej udostępnianej protokołami iSCSI/FC/FCoE;
        ii. Wsparcie dla podsystemu dyskowego w serwerze fizycznym – możliwość udostępniania urządzeń dyskowych zainstalowanych wewnątrz serwera indywidualnie, lub zwirtualiowanych i zabezpieczonych RAID – jako puli dyskowej dla platformy wirtualizacyjnej, do wykorzystania przez maszyny wirtualne.
5) Wsparcie dla możliwości bezpośredniego przekazywania do maszyn wirtualnych dysków wewnętrznych oraz wewnętrznych struktur RAID serwerów jako tzw. urządzenia dyskowe surowe lub jako kontrolery dyskowe w trybie tzw. pass-through

2. Systemy operacyjne dla maszyn wirtualnych w systemie wysokiej dostępności:

Na serwerach systemu wysokiej dostępności, w ramach zaoferowanej platformy wirtualizacyjnej należy uruchomić maszyny wirtualne z następującymi systemami operacyjnymi:

1) co najmniej 20 maszyn wirtualnych z systemami operacyjnymi z rodziny Linux – wskazanymi na etapie realizacji wdrożenia przez Zamawiającego – przy czym zakłada się, że są to systemy klasy enterprise (RedHat Linux Enterprise 8, Suse Linux Enterprise)
2) co najmniej 4 maszyny wirtualne z łącznie minimum 4 instancjami systemu Windows Server 2019

Oprogramowanie do wirtualizacji zaoferowane dla serwerów musi mieć architekturę i model licencyjny umożliwiające uruchomienie wyżej wymienionych maszyn wirtualnych z systemami operacyjnymi. Ponadto dla wymienionych systemów operacyjnych należy zaoferować licencję, subskrypcję i wsparcie pozwalające na ich wykorzystanie przez Zamawiającego przez minimum 5 lat, bez ponoszenia dodatkowych kosztów licencji, subskrypcji czy wsparcia.

B.I. Serwer fizyczny systemu baz danych NoSQL

Serwer fizyczny dla systemu baz danych NoSQL musi spełniać wszystkie wymagania zdefiniowane dla serwerów systemu wysokiej dostępności, oraz dodatkowe wymagania związane z koniecznością wykorzystania dysków magnetycznych (HDD) zainstalowanych wewnątrz serwera dla systemu baz danych NoSQL na potrzeby konfiguracji przestrzeni przechowywania danych dla silnika / systemu baz danych NoSQL.

Poniżej omówione wyłącznie specyficzne wymagania dla serwerów systemu baz danych NoSQL. Elementy wymagań wspólnych (dla serwerów systemu baz danych NoSQL oraz systemu wysokiej dostępności) pominięte w ramach definicji wymagań specyficznych dla serwerów systemu baz danych NoSQL oznaczono „[…]"

Wymagania te muszą być traktowane jako minimalne, chyba że treść wymogu w stanowi inaczej:

3. Pamięć masowa – podsystem dyskowy […] – należy dodatkowo uwzględnić wymagania:

1. **Zatoki na dyski magnetyczne/talerzowe/rotacyjne** – zwane dalej HDD – dla danych produkcyjnych:
    1. Minimalna liczba zatok na dyski HDD: **8**
    2. Minimalna liczba zainstalowanych dysków HDD: **4**
    3. Wsparcie *hot-swap* dla zatok wymaganych do obsadzenia min. 10 dysków HDD: TAK
2. […]
3. […]
4. **Dyski magnetyczne HDD** - dla danych systemu baz danych noSQL:
    1. Minimalna katalogowa pojemność dysku HDD [TB]: **2**
    2. Format dysku [cale]: 2.5 lub 3.5 cala
    3. Technologia i interfejs dysku: SAS
    4. Minimalna prędkość obrotowa [obr./min.]: 10 000
    5. Minimalna prędkość zapisu/odczytu danych w trybie nasyconym (blok 1MB) [MB/s]: 150
    6. Minimalna liczba operacji na sekundę [IOPS]: 150
    7. Minimalny bufor dla danych [MB]: 64
    8. Dysk klasy enterprise: Minimalny MTBF [godzin]: 2 000 000
    9. Wymagana dostępność 5-letniej gwarancji producenta na zaoferowany napęd: TAK
5. **Kontrolery dyskowe** / **kontrolery pamięci** SSD/NVMe
    1. […]
    2. Typy RAID wspierane przez kontrolery
        1. [...]
        2. Dla dysków HDD dla danych systemu baz danych NoSQL – wsparcie dla RAID5 i RAID6 oraz RAID10 a ponadto możliwość pracy w trybie tzw. JBOD / pass-through – tj. dostępu systemu operacyjnego lub platformy wirtualizacyjnej do każdego z dysków HDD z osobna (w celu realizacji struktur redundantnego przechowywania danych na poziomie silnika systemu baz danych NoSQL lub systemów operacyjnych serwerów systemu baz danych NoSQL)

B.II. Platforma wirtualizacyjna oraz systemy operacyjne serwerów systemu baz danych NoSQL

Dostarczenie platformy wirtualizacyjnej dla serwerów systemu baz danych NoSQL *jest opcjonalne i jest rozwiązaniem* ***dodatkowo punktowanym*** *– patrz opis kryterium technicznego „N".*

Platforma wirtualizacyjna uruchamiana na serwerach systemu baz danych NoSQL (jeśli dostarczona) musi spełniać wszystkie wymagania zdefiniowane dla platformy wirtualizacyjnej uruchamianej na serwerach systemu wysokiej dostępności (opisanej w punkcie A.II).

Na serwerach systemu baz danych – bezpośrednio lub w ramach zaoferowanej platformy wirtualizacyjnej – należy uruchomić następujące systemy operacyjne: co najmniej 6 instancji systemu operacyjnego z rodziny Linux – wskazanego na etapie realizacji wdrożenia przez Zamawiającego – przy czym zakłada się, że są to systemy klasy enterprise (RedHat Linux Enterprise 8, Suse Linux Enterprise). Dla uruchamianych systemów operacyjnych należy zaoferować licencję, subskrypcję i wsparcie pozwalające na ich wykorzystanie przez Zamawiającego przez minimum 5 lat, bez ponoszenia dodatkowych kosztów licencji, subskrypcji czy wsparcia.

C. Konsola / urządzenie KVM

Dla serwerów systemu wysokiej dostępności oraz serwerów systemu baz danych NoSQL musi zostać dostarczona jedna, wspólna konsola, spełniająca następujące wymagania:

1. wyposażona w składany monitor o przekątnej 17", z matrycą IPS o rozdzielczości 1920x1080 pkt.
2. wyposażona klawiaturę i touchpad oraz
3. Wysuwana, dostosowana do montażu w szafie rack 19"; wysokość 1U;

Wraz z konsolą należy dostarczyć urządzenie KVM o wysokości 1U, montowalny w szafie, umożliwiający:
1. dostęp z konsoli do wszystkich serwerów (systemu wysokiej dostępności i baz danych NoSQL);
2. przełączanie konsoli między źródłami (serwerami) bez modyfikacji połączeń fizycznych;
3. zdalne zarządzanie – poprzez zintegrowany w urządzeniu port 100Mbit/1Gbit Ethernet;

D. Szafy montażowe:

Elementy dostarczanej infrastruktury serwerowej (serwery, macierze, konsola, przełączniki sieć LAN/SAN dla infrastruktury serwerowej, system UTM, system wykonywania kopii zapasowych) muszą być zainstalowane w dostarczonych przez Wykonawcę szafach przemysłowych. Zakłada się instalację 3 szaf w Centrum Podstawowym i 1 szafy w Centrum Zapasowym. Każda z szaf musi spełniać poniższe wymagania:

1) Wymiary szafy:
   a) Wysokość użytkowa: 45U (wysokość zewnętrzna nie więcej niż 230 cm);
   b) Szerokość: 80 cm
   c) Głębokość: nie przekraczająca głębokości **100 cm** liczonej w podstawie szafy (jeśli drzwi wystają poza obrys szafy to nie należy uwzględniać drzwi w obrysie szafy)
2) Drzwi:
   a) drzwi frontowe oraz tylne: dwuskrzydłowe - dzielone 50%/50%;
   b) perforacja w stosunku do całej powierzchni drzwi musi być nie mniejsza niż 50%,
3) Wymiary szaf oraz sposób otwierania drzwi muszą być dobrane z uwzględnieniem zastrzeżeń / ograniczeń dotyczącymi głębokości i dostępu do szaf opisanymi w punkcie „opis miejsca instalacji" w SIWZ.
4) Zamykanie szafy: zamykane na klucz uniwersalny
5) Konstrukcja szafy:
   a) nośność szafy: 1500 kg,
   b) ściany boczne, z perforacją;
   c) dół szafy otwarty na całej powierzchni, szafa na cokole, nie dopuszcza się posadowienia na nóżkach;
   d) dach szafy – pełny, wyposażony w:
      i) przepusty: co najmniej 2 sztuki wyposażone w szczotki
      ii) wentylatory: w co najmniej 4 wentylatory oraz czujnik temperatur pozwalający na uruchamianie panelu przy przekroczeniu określonej wartości progowej temperatury wewnątrz szafy;
   e) belki podporowe stelaży w szafach należy ustawiać wszerz szafy czyli równolegle do frontu/tylu szafy (po długości 800 mm); jednocześnie belki te muszą umożliwiać montaż stelaży w różnych odległościach od frontu/tytuł szafy;
   f) Stelaż wewnętrzy szafy musi spełniać następujące wymagania:
      i) Odległość między osiami otworów montażowych w stelażach musi wynosić 46,5 cm.
      ii) Odległość między stelażami umożliwiającymi montaż urządzeń z uchwytami w rozstawie 19" (48,26 cm) musi wynosić 45 cm; odległość między stelażami od strony wewnętrznej musi umożliwiać montaż uchwytów serwerowych o rozstawie 48 cm,
      iii) Stelaż musi mieć kształt typu B lub S (kształt wąski przystosowany do montażu prowadnic serwerowych o zwiększonej wielkości podpór – stosunek szerokości frontu do szerokości profilu środkowego co najmniej jak 2,3 do 1) z otworami montażowymi wykonanymi od frontu oraz z boku profilu z trzema otworami montażowymi na każde 1U.
   g) Otwory montażowe:
      i) Otwory montażowe muszą być kwadratowe.
      ii) Wszystkie otwory montażowe od strony frontu szaf oraz tyłu szafy należy w widoczny sposób przyporządkować zgodnie z jednostką U (np. naklejka z miarą lub farbą).
6) Kolor szaf: RAL9005 (czarny);,
7) Maskownice boczne pomiędzy stelażem a bokiem szafy, każdy wyposażony co najmniej 2 profile szczotkowe o długości nie mniejszej 80 cm i szerokości nie mniejszej niż 90mm.,
8) Maskownice 1U – umożliwiające szybki montaż bez użycia śrub i narzędzi - w miejscach gdzie nie są zainstalowane serwery i inne elementy infrastruktury serwerowej

2. MACIERZ DYSKOWA (CENTRALNA)

Macierz dyskowa (centralna) dostarcza przestrzeń roboczą na pamięciach flash i dyskach magnetycznych dla danych systemowych, systemów operacyjnych, maszyn wirtualnych oraz aplikacji i baz danych działających na serwerach systemu wysokiej dostępnośc oraz serwerach system baz danych NoSQL.
Macierz świadczyć będzie usługi blokowe dla serwowania wolumenów dla maszyn wirtualnych w systemie wysokiej dostępności oraz opcjonalnie dla serwerów bazy danych NoSQL a także usługi plikowe (CIFS, NFS) – na potrzeby aplikacji i wymiany danych w ramach elementów infrastruktury serwerowej.
Dane składowane na macierzy zabezpieczone są poprzez redundantne składowanie w strukturach RAID oraz dodatkowo poprzez wykonywanie kopii zapasowych (za pośrednictwem platformy wirtualizacyjnej).

Macierz musi spełniać co najmniej poniższe wymagania dotyczące architektury, cech i funkcjonalności – przy czym wszystkie wymagania muszą być traktowane jako minimalne, chyba że treść wymogu stanowi inaczej.

2.a. Architektura macierzy dyskowej (centralnej)

1. Architektura macierzy dyskowej:

a) Macierz centralna (dyskowa) musi stanowić pojedyncze urządzenie wykorzystujące do składowania danych w trybie blokowym w tym *podsystem* pamięci flash (SSD/NVME) oraz *podsystem* pamięci HDD (dysków magnetycznych).
b) Niedopuszczalna jest realizacja pojedynczego systemu – macierzy dyskowej – w postacie wielu urządzeń połączonych przełącznikami lub wirtualizatorem sieci SAN, szyną SAS lub interfejsami PCIe.
c) Usługi plikowe mogą być realizowane przez oddzielne od macierzy dyskowej urządzenie tego samego producenta, dostosowane architekturą i parametrami do architektury i funkcjonalności oraz cech ilościowych i jakościowych podsystemu przechowywania blokowego. Usługi plikowe mogą być także realizowane w sposób zintegrowany z usługami przechowywania blokowego w jednym urządzeniu, **jednak nie jest dopuszczalne** rozwiązanie, w którym usługi protokołu *Fibre Channel* realizowane są w oparciu o **emulację protokołu FC** na wewnętrznym systemie plików urządzenia.
d) Pod**system** przechowywania blokowego macierzy musi składać się z co najmniej **dwóch kontrolerów pracujących w trybie wysokiej dostępności.** W przypadku awarii jednego kontrolera **systemu** przechowywania blokowego, inny kontroler automatycznie przejmuje jego funkcje i udostępnia klientom (hostom, serwerom) wszystkie zdefiniowane w podsystemie przechowywania blokowego wolumeny blokowe (dyskowe).
e) Pod**system** przechowywania plikowego macierzy musi składać się z co najmniej **dwóch kontrolerów** (głowic, węzłów, appliance, gateway) **pracujących w trybie wysokiej dostępności.** W przypadku awarii jednego kontrolera **systemu** przechowywania blokowego, inny kontroler automatycznie przejmuje jego funkcje i udostępnia klientom (hostom, serwerom, urządzeniom PC) wszystkie zdefiniowane w podsystemie przechowywania plikowego udziały sieciowe (NFS, CIFS).

2. Przestrzeń przechowywania danych macierzy dyskowej:

a) Macierz dyskowa musi zapewniać przestrzeń przechowywania danych na pamięciach flash (SSD, NVMe) o pojemności użytkowej minimum **50TiB**. Wymagana sumaryczna minimalna pojemność użytkowa przestrzeni przechowywania danych na pamięciach flash (SSD/NVMe) musi być uzyskana przy pomocy **minimum 20 identycznych napędów/modułów flash (SSD/NVMe).**
b) Macierz dyskowa musi zapewniać przestrzeń przechowywania danych na dyskach magnetycznych (HDD) o pojemności użytkowej minimum **200TiB**. Wymagana sumaryczna minimalna pojemność użytkowa przestrzeni przechowywania danych na dyskach magnetycznych (HDD) musi być uzyskana przy pomocy **minimum 100 identycznych napędów/dysków magnetycznych (HDD).**
a) *Uwaga! Zaoferowanie macierzy, której przestrzeń przechowywania na dyskach magnetycznych (HDD) ma pojemność użytkową większą niż 200TiB jest **dodatkowo punktowane** (patrz opis kryterium H).*
b) Zaoferowana macierz dyskowa musi być **rozbudowywalna** do sumarycznej pojemności użytkowej przestrzeni przechowywania danych na dyskach magnetycznych (HDD) **minimum 600TiB** poprzez wyłącznie dodawanie napędów / dysków magnetycznych (HDD), tego samego typu (technologia, wielkość fizyczna, pojemność katalogowa) jak zaoferowane w macierzy.

2.b. Cechy i funkcjonalność macierzy dyskowej (centralnej)

1. Wydajność macierzy:

a) **Podsystem pamięci flash (SSD/NVMe):**

i) wydajność zapisu i odczytu losowego danych w przestrzeni przechowywania na pamięciach flash (SSD/NVME), dla bloków I/O o wielkości 4kB lub 8kB przy stosunku 60%/40% i więcej (do 75%/25%) odczytów do zapisów – **nie mniej niż 370 000 IOPS;**

b) **Podsystem pamięci magnetycznych (HDD):**

i) wydajność zapisu i odczytu strumieniowego danych w przestrzeni przechowywania na dyskach magnetycznych (HDD) dla bloków I/O o wielkości 64kB i większych (do 1MB per blok I/O), przy - odpowiednio 100% zapisów oraz 100% odczytów - **nie mniej niż 3 GB/s;**

c) **Wydajność – sposób mierzenia wydajności:**

i) **Wydajność** zaoferowanej macierzy w zaoferowanej konfiguracji – **należy udokumentować,** poprzez załączenie do oferty wyników testu wydajnościowego macierzy przeprowadzonego zgodnie z dobrymi praktykami w zakresie testów wydajności – oddzielnie dla pomiaru wydajności w IOPS operacji zapisu i odczytu danych na pamięciach flash (SSD/NVMe) oraz dla pomiaru wydajności w MB/s operacji zapisu i odczytu danych na dyskach magnetycznych (HDD); uwaga! wyn*iki testu wydajnościowego załączone do oferty muszą zawierać – poza wartościami liczbowymi uzyskanymi dla testów wydajności macierzy muszą zawierać także: opis środowiska testowego w tym: konfiguracji macierzy (producent/model/typ, liczba i typ kontrolerów, pojemność pamięci cache macierzy, liczba serwerów testujących wydajność macierzy, pojemność pamięci RAM tych serwerów, nazwa narzędzia testującego oraz użyte parametry testu, w szczególności rozmiar danych / wolumenu testowego i/lub czas wykonania testu, wielkość bloku I/O dla poszczególnych testów i liczba wątków testu wydajnościowego);*

ii) Załączone do oferty wyniki testów wydajnościowych muszą być możliwe do uzyskania w zaoferowanej konfiguracji macierzy;

iii) *Wynik testu wydajnościowego załączonego do oferty nie musi być podany dla identycznej konfiguracji macierzy dyskowej jak konfiguracja, która została zaoferowana, jednak konfiguracja wykorzystana do testów wydajnościowych musi być zbliżona do zaoferowanej macierzy dyskowej pod względem liczby i rodzaju kontrolerów dyskowych, liczby i rodzaju napędów pamięci flash (SSD/NVMe) i napędów dyskowych (HDD) oraz liczby i rodzajów interfejsów sieciowych macierzy do serwerów (np. FC vs Ethernet); w szczególności nie będą akceptowane wyniki testu:*

(1) uzyskane dla macierzy w konfiguracji z przeważającą lub wyłączną przestrzenią na pamięciach flash (SSD/NVMe) i/lub z włączonym buforowaniem dysków magnetycznych za pomocą cache wykorzystującego pamięci flash (SSD/NVMe) podane jako wyniki testu wydajnościowego dla przestrzeni na dyskach magnetycznych (HDD) w technologii SAS;

(2) uzyskane dla macierzy w konfiguracji o wielokrotnie większej liczbie modułów pamięci flash (SSD/NVMe) czy napędów dyskowych niż zaoferowana macierz (dopuszcza się wyniki testów dla liczby napędów lub dysków większej o maksymalnie 50% niż w zaoferowanej macierzy);

(3) uzyskane dla wolumenu danych testowych mniejszego niż dwukrotność sumy pojemności pamięci cache macierzy i pojemności pamięci operacyjnej RAM w serwerach testujących;

iv) *Sposób prezentacji wyników testów wydajnościowych macierzy oraz konfiguracja macierzy wykorzystana do testu wydajnościowego zaprezentowanego jako dokumentacja wydajności macierzy musi zapewniać możliwość* weryfikacji deklarowanych w ofercie parametrów wydajnościowych macierzy, np. poprzez ich porównanie z referencyjnymi, dostępnymi publicznie wynikami testów rozwiązań macierzowych wykonywanych przez niezależne organizacje np.:

(1) Dla wydajności zapisu i odczytu losowego danych blokiem I/O 4/8kB w przestrzeni przechowywania na pamięciach flash (SSD/NVME) – wyniki testu SPC-1 dostępne na stronie: (https://spcresults.org/benchmarks/results/spc1-spc1e)

(2) Dla wydajności zapisu i odczytu sekwencyjne danych blokiem I/O 64kB i większym w przestrzeni przechowywania na dyskach magnetycznych (HDD) – wyniki testu SPC-2 dostępne na stronie: (https://spcresults.org/benchmarks/results/spc2-spc2e)

v) Zastrzega się, że w przypadku stwierdzenia przez Zamawiającego wątpliwości dotyczących interpretacji lub wiarygodności wyników testów wydajnościowych macierzy załączonych do oferty to na *Wykonawcy spoczywa ciężar udowodnienia, że załączone do oferty wyniki testów wydajnościowych są wiarygodne i właściwe dla wydajności macierzy w zaoferowanej konfiguracji;*

vi) Zamawiający zastrzega sobie prawo weryfikacji wydajności macierzy dyskowej po dostarczeniu macierzy do siedziby Zamawiającego, w ramach testów akceptacyjnych przedmiotu zamówienia. Zamawiający zastrzega sobie także prawo wezwania Wykonawcy do przeprowadzenie testów wydajnościowych dostarczonej macierzy obecności i pod nadzorem Zamawiającego

2. Niezawodność:

a) **Redundancja danych**: Podsystem przechowywania blokowego macierzy centralnej musi zapewniać redundancję przechowywanych danych minimum na następujących poziomach:

i) Dla przestrzeni przechowywania danych na pamięciach flash (SSD, NVMe): RAID1, RAID10

ii) Dla przestrzeni przechowywania danych na dyskach magnetycznych (HDD): RAID 1, RAID10 a także RAID5 oraz RAID6 lub równoważny (podwójna parzystość, np. RAID-DP itp.)

b) Macierz dyskowa musi wspierać (na poziomie architektury i funkcjonalności) **replikację danych między macierzami tego samego producenta**, na bazie wewnętrznych mechanizmów macierzy; funkcjonalność ta nie musi być dostarczona, nie jest także wymagana licencja na tę funkcjonalność.

c) **Odporność zasobów dyskowych na awarie, wielościeżkowy dostęp do danych:**

i) Macierz musi wspierać niezależny restart lub awarię jednego z redundantnych kontrolerów zasobu SSD/NVMe, bez przerywania dostępu do zasobu SSD/NVMe z punktu widzenia serwerów dla meta-danych korzystających z tego zasobu.

ii) Macierz, tj. moduł kontrolera i obudowy pamięci/modułów pamięci flash SSD/NVMe oraz dysków magnetycznych muszą być wyposażone w redundantne zasilacze i wentylatory. W każdym z modułów, redundantne zasilacze muszą mieć możliwość zasilania z różnych źródeł, bez potrzeby użycia zewnętrznych urządzeń.

iii) Jeśli jest to konieczne, dla macierzy dyskowej muszą zostać dostarczone licencje na funkcję umożliwiającą wykorzystywanie kontrolerów macierzy w taki sposób, aby oprogramowanie zainstalowane w systemie operacyjnym klienta (hosta) lub oprogramowanie platformy wirtualizacyjnej dla serwerów automatyczne przełączało ścieżki do zasobów, np. w przypadku uszkodzenie karty HBA, przełącznika SAN, kontrolera macierzy czy kabla optycznego;

iv) Jeśli jest to konieczne, wraz z macierzą muszą zostać dostarczone licencje umożliwiające równoczesne wykorzystanie wielu ścieżek w sieci SAN między hostem a macierzą dyskową; Licencje te muszą zostać dostarczone dla platformy wirtualizacyjnej zaoferowanej dla systemu wysokiej dostępności oraz dla systemów operacyjnych Windows Server 2019, RedHat Linux Enterprise 8, Suse Linux Enterprise..

d) **Funkcje hot-swap oraz aktualizacja firmware:**

i) Macierz musi umożliwiać wymianę napędów/modułów pamięci flash (SSD/NVMe) oraz dysków magnetycznych (HDD) na gorąco, tj. bez konieczności wyłączania całej macierzy lub puli, w której awarii uległ napęd lub struktury redundantnego przechowywania danych (RAID) w której uległ awarii napęd, a także bez potrzeby wyłączania półki, obudowy lub tacki zawierającej więcej niż 1 napęd/moduł SSD/NVMe lub 1 dysk magnetyczny (HDD);

ii) Macierz musi umożliwiać aktualizację firmware kontrolerów macierzy na gorąco, bez przerywania dostępu do wolumenów dyskowych perspektywy serwerów (hostów);

3. Funkcjonalność macierzy dyskowej:

a) **Podstawowe funkcje i mechanizmy macierzy dyskowej:**

i) *Mapowanie wolumenów:*

(1) Macierz dyskowa musi umożliwiać mapowanie wolumenów do hostów, w taki sposób, że **możliwy jest przydział numerów LUN niezależnie dla minimum 28 hostów lub grup hostów**, przy uwzględnieniu warunku, że numery mogą być przydzielane dowolnie od 0 do maksymalnej wartości. Przykładowo, dla każdego z hostów lub grup hostów musi istnieć możliwość mapowania oddzielnego wolumenu o numerze LUN 0,

(2) Macierz dyskowa musi umożliwiać wirtualizację nazewnictwa hostów lub grup hostów poprzez nadawanie tzw. *aliasów tekstowych*, widocznych globalnie na każdym kontrolerze zasobu. Musi istnieć możliwość stworzenia aliasów tekstowych hostów lub grup hostów złożonych co najmniej z następującego zbioru znaków ASCI: 0-9, a-z, A-Z.

(3) Macierz dyskowa musi umożliwiać udostępnianie wolumenów dyskowych **co najmniej 20 serwerom** z zainstalowaną platforma wirtualizacyjną oraz dodatkowo co najmniej 20 serwerom z systemem operacyjnym z rodziny Linux. W przypadku licencjonowania liczby hostów podłączanych do macierz dyskowej należy dostarczyć odpowiednie licencje.

(4) Macierz dyskowa musi umożliwiać udostępnianie hostom wolumenów większych niż 2TB;

ii) ***Funkcje do zarządzania:***

(1) Dostęp do kontrolerów macierzy dyskowej lub do graficznego interfejsu zarządzania i monitorowania zasobu musi być możliwy poprzez sieć Ethernet oraz TCP/IP, z komputera PC pracującego pod kontrolą systemu operacyjnego z rodziny MS Windows i Linux.

(2) Macierz dyskowa musi umożliwiać prezentację obciążenia przy pomocy dostarczonego oprogramowania lub poprzez interfejs webowy w czasie rzeczywistym; oprogramowanie do monitorowania wydajności może być integralną częścią kontrolerów zasobu lub może być zainstalowane na dedykowanym serwerze zewnętrznym (w takim wypadku należy dostarczyć taki serwer do zarządzania macierzą);

b) **Zaawansowane funkcje i mechanizmy macierzy dyskowej:**

i) *Rozkładanie obciążenia I/O na wielu dyskach:*

(1) Macierze musi umożliwiać konfigurację wielu dysków w jednej puli i równomiernego rozkładania zapisów i odczytów na wszystkie dyski w puli;
(2) nie jest wymagana funkcjonalność *wide-striping* dla wszystkich dysków macierzy jednakże macierz posiadająca taką funkcjonalność spełnia w/w kryterium, pod warunkiem dostarczenia licencji dla tej funkcjonalności na całą pojemność macierzy, jeśli taka licencja jest wymagana (a także dla powiększonej pojemności macierzy – jeśli takie rozszerzenie pojemności macierzy jest dostarczane – zgodnie z kryterium technicznym „H";

ii) *Thin provisioning*:
(1) Dostarczone rozwiązanie musi mieć możliwość dynamicznego alokowania przestrzeni przechowywania danych w macierzy dyskowej (tzw. ang. *thin-provisioning)* minimum dla wolumenów blokowych serwowanych do serwerów systemu wysokiej dostępności;
(2) Jeżeli funkcjonalność *thin provisioning* jest zrealizowana na poziomie macierzy dyskowej oraz wymaga dodatkowej licencji, to należy taka licencję uwzględnić w ofercie, przy czym dostarczona licencja dla *thin-provisionong* musi obejmować pełną pojemność macierzy, (a także powiększoną pojemność macierzy – jeśli takie rozszerzenie pojemności macierzy jest dostarczane – zgodnie z kryterium technicznym „H");
(3) Jeśli zaoferowana macierz dyskowa nie posiada funkcjonalności *thin provisioning* to macierz musi być kompatybilna z rozwiązaniem do wirtualizacji serwerów zaoferowanym dla systemu wysokiej wydajności, zapewniającym realizację funkcjonalność *thin-provisioning* na poziomie platformy wirtualizacyjnej i taka funkcjonalność musi być dostarczona dla tej platformy;

iii) *Automatyczne buforowanie danych na pamięciach flash*
(1) Macierze musi umożliwiać konfigurację wolumenów blokowych w taki sposób, że dane składowane na pulach dysków magnetycznych (HDD) będą automatycznie buforowane na pulach pamięci flash / SSD w sposób konfigurowalny przez użytkownika jednakże sterowany przez kontroler macierzy, np. na podstawie schematu dostępu do danych (ang. *I/O pattern*);
(2) Jeżeli funkcjonalność *automatycznego buforowania danych na pamięciach flash* wymaga dodatkowej licencji, to należy taka licencję uwzględnić w ofercie, przy czym dostarczona licencja musi obejmować pełną pojemność macierzy (a także powiększoną pojemność macierzy – jeśli takie rozszerzenie pojemności macierzy jest dostarczane – zgodnie z kryterium technicznym „H");;
(3) Dostarczenie mechanizmu *auto-tiering* dla macierzy nie jest wymagane, jednakże macierz wspierająca mechanizm *auto-tiering* spełnia w/w kryterium, pod warunkiem dostarczenia licencji dla tej funkcjonalności na całą pojemność macierzy (a także powiększonej pojemności macierzy – jeśli takie rozszerzenie pojemności macierzy jest dostarczane – zgodnie z kryterium technicznym „H");, jeśli taka licencja jest wymagana;
(4) Wsparcie przez macierz buforowania danych składowanych na pulach dysków magnetycznych (HDD) w wewnętrznej pamięci podręcznej (cache) kontrolerów macierzy dyskowej nie jest równoznaczny ze spełnieniem w/w wymogu wsparcia dla *automatycznego buforowania danych na pamięciach flash; istota wymaganej funkcjonalności polega na wykorzystaniu przestrzeni pamięci flash (SSD/NVMe) w dostarczonej macierzy do buforowania danych składowanych na dyskach magnetycznych, która to przestrzeń ma wielokrotnie większą pojemność niż typowa pojemność pamięci cache w kontrolerach macierzy (rzędu wielu TB vs rzędu GB/pojedynczych TB);*

4. Certyfikacja/zgodność:

a) *Zgodność z RoHS*
b) *Zgodność z deklaracją CE*
c) *Macierz dyskowa musi być obecna na liście kompatybilności systemów: VMware vSphere 7, RedHat Virtualization oraz RedHat Enterprise Linux 8, Suse Enterpise Linux Server 15 i Windows Server 2019*
d) Dla wymienionych w ppkt. c) środowisk wirtualizacyjnych oraz systemów operacyjnych macierz musi umożliwiać realizację wielościeżkowego dostępu do danych zapewniające wysoką niezawodność dostępu hostów do macierzy (przełączanie ścieżek komunikacyjnych w przypadku awarii portów, przełączników lub ścieżek w sieci SAN) oraz równoważenie obciążenia ścieżek komunikacyjnych między hostami i macierzą dyskową; rodzaj i liczba dostarczonych licencji na funkcjonalność wielościeżkowego dostępu musi być odpowiednia dla zaoferowanych serwerów sytemu wysokiej dostępności i systemu baz danych NoSQL oraz ich oprogramowania wirtualizacyjnego i systemowego;
e) Producent macierzy dyskowej musi być odnotowywany w zestawieniach i raportach uznanych organizacji działających w sektorze usług i systemów IT, w tym minimum: w raportach firmy Gartner za lata 2018, 2019 i 2020; dla roku 2020 należy odnosić się do raportu p.n. „Magic Quadrant for Primary Storage Arrays" (adres dostępowy do dokumentu z raportem – data pobrania 20.12.2020: https://www.gartner.com/doc/reprints?id=1-24PF3N7Q&ct=201201&st=sb);

2.c. Komponenty macierzy dyskowej (centralnej)

1. Kontrolery macierzy:

a) **Pamięć cache:**
   i) Macierz dyskowa musi posiadać pamięć cache wykorzystywaną na potrzeby buforowania danych o pojemności fizycznej co najmniej **64 GB** na całą macierz; każdy z kontrolerów składających się na zasób musi posiadać proporcjonalną do całości ilość pamięci.
   ii) Macierz dyskowa musi realizować mirroring pamięci cache między kontrolerami oraz mechanizm gwarantujący zachowanie zawartości pamięci cache w przypadku zaniku zasilania;

b) **Porty komunikacyjne:**
   i) Macierz musi być wyposażona w co najmniej 8 interfejsów I/O w technologii FC, o przepustowości minimum 16Gbit/s, do przyłączenia macierzy do infrastruktury SAN, w celu realizacji usług blokowego przechowywania i dostępu do danych
   ii) Macierz musi być wyposażona w co najmniej 4 interfejsów I/O w technologii 10 Gbit Ethernet lub szybszej, do przyłączenia macierzy do infrastruktury LAN, w celu realizacji usług plikowego przechowywania i dostępu do danych
   iii) Ponadto macierz musi posiadać co najmniej 2 porty sieci LAN (Ethernet, miedź) do zarządzania;

2. Podsystem pamięci flash (SSD/NVMe);

a) **Napędy/moduły flash (SSD/NVMe) zastosowane w macierzy dyskowej:**
   i) Muszą być wykonane w technologii SSD (typu SLC lub MLC) lub NVMe
   ii) Interfejsy: SAS lub PCIe
   iii) Automatyczne monitorowanie stanu napędów i określanie stopnia zużycia mediów.
   iv) Minimalna pojemność pojedynczego napędu/modułu: 3TB
   v) Minimalna przepustowość pojedynczego napędu/modułu:
      (1) Liczba operacji zapisu na sekundę, blok I/O 4kB [IOPS]: 100 000
      (2) Liczba operacji odczytu na sekundę, blok I/O 4kB [IOPS]: 200 000
      (3) Prędkość zapisu sekwencyjnego (blok 1MB) [MB/s]: 1000
      (4) Prędkość odczytu sekwencyjnego (blok 1MB) [MB/s]: 2000
   vi) Napędy muszą być typu serwerowego, klasy enterprise, MTBF minimum 2 mln godzin
   vii) Odporność na ścieranie: minimum 3.0 DWPD
   viii) Maksymalne opóźnienie operacji zapisu dla pojedynczego napędu SSD [mikrosekund]: 4

b) Macierz musi realizować mechanizm balansowania zużycia pamięci SSD/NVMe (ang. wear-leveling)

c) Macierz musi wykrywać i raportować stan zużycia pamięci SSD/NVMe (tzw. ścieranie)

3. Podsystem pamięci magnetycznych (HDD);

a) **Dyski magnetyczne (HDD) zastosowane w macierzy dyskowej:**
   i) Minimalna pojemność surowa katalogowa dysku: **12TB**
   ii) Technologia dysku: SAS lub FC
   iii) Wydajność pojedynczego dysku:
      (1) Minimalna liczba operacji I/O na sekundę przy wielkości bloku 4kB [IOPS]: 170
      (2) Minimalna przepustowość dysku dla zapisu i odczytu sekwencyjnego (blok 1MB) [MB/s]: 230
      (3) Maksymalne opóźnienie [ms]: 4.5
   iv) Dysk klasy enterprise, MTBF: minimum 2 000 000
   v) Napędy muszą być typu serwerowego, klasy enterprise, z MTBF minimum 2 mln godzin

b) Macierz musi monitorować i prezentować dane z systemu SMART dysków magnetycznych (HDD), w szczególności musi alarmować o przekroczeniu wartości progowych związanych z niezawodnością

4. Podsystem plikowy:

a) Podsystem plikowy musi realizować usługi plikowe co najmniej dla protokołów NFS v3 i v4 oraz CIFS

b) Podsystem plikowy musi mieć wydajność:
   i) Sekwencyjnego zapisu/odczytu danych (z blokiem 64kB i większym) - co najmniej **1 GB/s;**
   ii) Losowego zapisu/odczytu danych (z blokiem 4kb lub 8kB) - co najmniej **50 000 IOPS**

c) Procesory podsystemu plikowego nie mogą równocześnie z obsługą protokołów plikowych realizować usług przechowywania blokowego macierzy dyskowej (np. wyliczać dane dla struktur RAID itp.);

d) Podsystem plikowy musi być zaoferowany w konfiguracji zapewniającej niezawodność i odporność na awarię pojedynczych komponentów, w szczególności kontrolerów podsystemu plikowego realizujących usługi przechowywania plikowego i plikowego dostępu do danych; redundantne kontrolery podsystemu plikowego muszą realizować mechanizmy wysokiej niezawodności w trybie active-active; umożliwiające przejmowanie obsługi zasobów plikowych przez działający kontroler (kontrolery) w przypadku awarii jednego (lub 50%) kontrolerów podsystemu plikowego;

3. MACIERZ OBIEKTOWA

Macierze obiektowe pełnią kluczową rolę w projektowanej infrastrukturze serwerowej Biblioteki Śląskiej – zapewniają długofalowe, wiarygodne i odporne na awarie przechowywanie zdigitalizowanych zbiorów. Stanowią one docelowe miejsce trwałego przechowywania w infrastrukturze serwerowej danych zdigitalizowanych obiektów cyfrowych. Dane obiektów cyfrowych pozyskiwane, przetwarzane, edytowane i udostępniane w projektowanej infrastrukturze serwerowej, z wykorzystaniem aplikacji, platform i środowisk działających w systemie wysokiej dostępności, systemie baz danych NoSQL oraz korzystających z zasobów macierzy dyskowej (centralnej) będą –w formie gotowej do archiwizacji (tj. spakowane w archiwa opatrzone meta-danymi, zapisane w odpowiednim formacie, zgodnym ze dziedzinowymi standardami, np. OAIS[1,2]), – umieszczane w dwóch macierzach obiektowych, rozmieszczonych w dwóch rozłącznych lokalizacjach, tj. serwerowniach Centrum Podstawowego i Centrum Zapasowego Biblioteki Śląskiej, połączonych dedykowanym łączem sieciowym o odpowiedniej przepustowości.
Rozproszone geograficznie macierze obiektowe stanowić będą wysoko-pojemne i bezpieczne repozytorium zapewniające bezpieczeństwo fizyczne i logiczne oraz trwałość i niezmienność zdeponowanych danych. Takie cechy archiwum obiektowego zostaną osiągnięte poprzez realizację mechanizmów wielopoziomowego zabezpieczenia danych, w tym geograficznej replikacji danych i lokalnego nadmiarowego przechowywania danych (kodowanie nadmiarowe, ang. *Erasure Coding)* oraz automatycznej kontroli integralności danych, wykrywania i korekcji błędów w danych, proaktywnego monitorowania nośników danych (w tym dysków twardych macierzy obiektowych) a także poprzez zapewnienie wsparcia dla funkcjonalności WORM.
Specyfika działań digitalizacyjnych w ramach Śląskiej Biblioteki Cyfrowej nie wymaga od macierzy obiektowych replikacji synchronicznej. Dane generowane są każdorazowo wyłącznie w Centrum Podstawowym, gdzie znajduje się źródło danych (pracownia digitalizacyjna) a także macierz (dyskowa centralna), system wysokiej dostępności i system baz danych NoSQL, na których działają usługi i aplikacje wspierające proces digitalizacji, edycji, przygotowania do publikacji, prezentacji danych oraz agregacji meta-danych. Biblioteka Śląska nie realizuje aplikacji krytycznych (ang. *mission-critical*), w których wymagany jest ścisły reżim replikacji danych do drugiego centrum danych. Replika danych z macierzy obiektowej w Centrum Podstawowym wykonywana na macierz obiektową w Centrum Zapasowym stanowi zabezpieczenie na wypadek awarii Centrum Podstawowego. Mogą być tolerowane w tym środowisku chwilowe niespójności obrazu zawartości obu replik archiwum obiektowego znajdujących się w poszczególnych serwerowniach – dopuszczalny jest model spójności tzw. *eventual consistency*. Analogicznie, nie jest wymagane wsparcie dla mechanizmów niezawodności *active-active*. Dane archiwalne „produkowane" są wyłącznie w Centrum Podstawowym, a przełączenie obsługi archiwum obiektowego na Centrum Zapasowe może odbywać się z niewielkim opóźnieniem; nie jest także wymagane równoczesne wykorzystanie obu macierzy obiektowych do składowania lub odczytu danych archiwalnych. Nie zakłada się też replikacji czy przenoszenia awaryjnego wszystkich procesów Biblioteki Cyfrowej do Centrum Zapasowego, m.in. ze względu na specyfikę digitalizacji prowadzonej w podstawowej lokalizacji Biblioteki, w tym jej ścisłego związku ze sprzętem digitalizacyjnym.
Macierze obiektowe udostępniać będą interfejsy obiektowe (minimum S3) i plikowe (minimum NFS a także, opcjonalnie, CIFS/SMBFS) w celu zapewnienia zgodności rozwiązania do przechowywania długoterminowego danych z obecnie wykorzystywanymi i przyszłymi narzędziami, platformami i usługami, w tym repozytoriami cyfrowymi, serwerami treści cyfrowych, narzędziami do zarządzania archiwizacją danych itp.
Wymagane wsparcie dla protokołu S3 ma znaczenie operacyjne (kompatybilność z systemami zewnętrznymi omówiona powyżej); jest także środkiem zapobiegawczym przeciwko skutkom starzenia się technologii. Długofalowo, jednym ze sposobów zabezpieczenia zbioru danych składowanych w określonym systemie przed skutkami starzenia się technologii jest zapewnienie wsparcia w tym produkcie standardowych, powszechnie wykorzystywanych protokołów dostępu do danych i meta-danych, co umożliwi migrację danych w przyszłości poza dany produkt. Dla systemów obiektowych takim standardowym protokołem jest przede wszystkim S3 (ang. *Amazon Simple Storage Service*), który jest szeroko wspierany w chmurze publicznej i macierzach obiektowych.

Przez **system macierzy obiektowych** rozumie się dwie, współpracujące macierze obiektowe, rozlokowane w dwóch serwerowniach Biblioteki Śląskiej, wzajemnie replikujące składowane w nich dane, a dodatkowo realizujące lokalnie zabezpieczenie danych przez redundantne (nadmiarowe) składowanie danych w obrębie każdej z serwerowni a także przejmujące obsługę ruchu związanego ze składowaniem i dostępem do danych oraz żądań I/O użytkowników, platform i aplikacji klienckich działających w systemie wysokiej dostępności w przypadku awarii jednej z macierzy obiektowych składających się na system macierzy obiektowych.

1 http://www.oais.info/
2 https://public.ccsds.org/pubs/650x0m2.pdf

Macierze obiektowe muszą spełniać co najmniej poniższe wymagania wysokopoziomowe i szczegółowe dotyczące architektury, cech i funkcjonalności systemu macierzy obiektowych – przy czym wszystkie wymagania muszą być traktowane jako minimalne, chyba że treść wymogu stanowi inaczej**.**

3.a. Architektura, cechy i funkcjonalność wysokopoziomowa macierzy obiektowej:

1) **Architektura wysokopoziomowa systemu macierzy obiektowych:**
   a) Macierze obiektowe muszą być zintegrowanym, złożonym z oprogramowania oraz komponentów sprzętowych systemem wysokodostępnym, skalowalnym w zakresie pojemności i wydajności przechowywania danych, posiadającym rozszerzalną architekturę typu *scale-out*,
   b) Macierze obiektowe muszą być zrealizowane w oparciu o komponenty sprzętowo-programowe, jako tzw. *appliance* – tj. rozwiązanie będące połączeniem sprzętu i oprogramowania tego samego producenta (dopuszczalny jest także tzw. OEM), oferowane przez producenta jako zintegrowane rozwiązanie występujące w katalogu producenta oraz jego cenniku.
   c) Macierz obiektowa musi składać się z węzłów (serwerów, appliance) połączonych redundantną siecią komunikacyjną, realizujących mechanizmy niezawodności, w tym redundancji przechowywania danych, korekcji danych oraz przełączania obsługi żądań I/O pomiędzy węzłami macierzy obiektowej;
   d) Pojedyncza macierz obiektowa musi stanowić w pełni funkcjonalny, niezależny od drugiej macierzy obiektowej system przechowywania obiektowego. *Wymagana jest całkowita niezależność działania każdej z macierzy obiektowych od drugiej macierzy obiektowej w tym możliwość dostępu do składowanych w macierzy danych i meta-danych a także możliwość zapisu / składowania nowych danych do macierzy niezależnie od awarii drugiej z macierzy.*
   e) Nawet całkowita awaria jednej z macierzy obiektowych a także rozległa awaria w jednej z serwerowni Biblioteki Śląskiej (w Centrum Podstawowym lub w Centrum Zapasowym) nie może uniemożliwiać składowania i dostępu do danych przechowywanych w systemie macierzy obiektowych. Jeżeli do zapewnienia takiej funkcjonalności konieczne jest zastosowanie mechanizmów niezawodności na tzw. front-end macierzy obiektowych, to taki mechanizm musi zostać przewidziany i zapewniony przez Wykonawcę w ramach dostawy i wdrożenia systemu macierzy obiektowych.
   f) Replikacja danych z Centrum Podstawowego do Centrum Zapasowego nie może być zrealizowana w ramach pojedynczej (logicznie) macierzy obiektowej – wymagane jest zapewnienie redundantnego z perspektywy lokalnego centrum danych przechowywania w każdej z macierzy obiektowej a także dodatkowo replikacji geograficznej przechowywanych lokalnie danych;
   g) Każda macierz obiektowa (w każdym z ośrodków) **musi składać się z minimum 8 węzłów** (serwerów, appliance) w celu minimalizacji wpływu awarii węzłów macierzy na poziom zabezpieczenia danych oraz wydajność składowania i dostępu do danych w macierzy obiektowej;

2) **Funkcjonalność i cechy wysokopoziomowe systemu macierzy obiektowych:**
   a) System macierzy obiektowych musi realizować obiektowe przechowywanie danych, w sposób zapewniający długofalowe, bezpieczne i trwałe przechowywanie oraz dostęp do danych, poprzez m.in. zabezpieczenie logiczne i fizyczne danych, w tym wsparcie dla mechanizmów zabezpieczających dane przed modyfikacją oraz replikację geograficzną danych i lokalne przechowywanie redundantne danych.
   b) Macierz obiektowa musi umożliwiać elastyczne konfigurowanie poziomu redundancji przechowywania danych w strukturach opartych o tzw. kodowanie nadmiarowe (tzw. ang. *Erasure Coding*), w tym możliwość wskazywania poziomu odporności macierzy obiektowej na awarię określonej liczby komponentów takich jak węzły (serwerów, appliance) macierzy obiektowej i/lub napędy dyskowe.
   c) *Nie są akceptowane rozwiązania, w których lokalne przechowywanie nadmiarowe danych jest realizowane przez zastosowanie struktur RAID, typowych dla klasycznych macierzy dyskowych;*
   d) *Nie są akceptowalne rozwiązania, w których redundancja przechowywania danych na poziomie lokalnym lub geograficznym jest realizowana mechanizmami systemu plików czy to wewnętrznego, implementowanego w kontrolerach macierzy dyskowych lub serwerów plików czy to zewnętrznego – nie zaś mechanizmami wbudowanymi w system przechowywania obiektowego;*
   e) Pojedyncza macierz obiektowa musi wspierać poziom niezawodności zapewniający minimum:
      i) **odporność na awarię 2 węzłów** (serwerów, *appliance*) macierzy obiektowej w danym ośrodku;
      ii) **odporność na awarię 10% napędów dyskowych** w ramach każdej z macierz obiektowych;
   f) System macierzy obiektowych musi gwarantować **odporność** danych na następujące zagrożenia:
      i) awarie sprzętu oraz lokalne zdarzenia mogące uszkodzić dane – poprzez realizację wielopoziomowych zabezpieczeń fizycznych danych (replikacja, składowanie nadmiarowe);
      ii) błędy aplikacji oraz błędy użytkowników a także ataki wirusów i hackerów – poprzez wsparcie m.in. dla wersjonowania danych oraz mechanizmów zabezpieczających przed modyfikacją danych;

iii) starzenie się technologii przechowywania danych w tym mediów, technologii serwerowych i oprogramowania systemu obiektowego – poprzez wsparcie standardowych protokołów dostępu do składowanych danych i meta-danych, w tym minimum Amazon S3 – w zakresie umożliwiającym masową migrację danych z systemu macierzy obiektowych z/do innych systemów zewnętrznych;

g) **Wielodostęp, skalowalność**
   i) System macierzy obiektowych musi mieć architekturę wysokodostępną, bez pojedynczego punktu awarii w środowisku lokalnym i rozproszonym geograficznie na min. dwie lokalizacje (CP i CZ);
   ii) architektura systemu musi umożliwiać przełączenie obsługi żądań I/O (składowanie i dostęp do danych, operacje na meta-danych, listowanie kontenerów, listowanie atrybutów obiektów) pomiędzy węzłami macierzy w ramach centrum danych oraz między centrami danych;
   iii) Architektura rozwiązania musi być skalowalna – macierz obiektowa musi być rozszerzalna zarówno poprzez tzw. skalowanie wertykalne (rozszerzanie poszczególnych komponentów, np. pojemności węzłów systemu obiektowego lub wydajności elementów sieci) jak i skalowanie horyzontalne (dodawanie komponentów/węzłów systemu obiektowego lub sieci);
   iv) Przestrzeń przechowywania macierzy obiektowej musi być **rozszerzalna do minimum 100 PiB** pojemności logicznej;
   v) Przestrzeń adresowa macierzy obiektowej musi umożliwiać zarządzanie, przechowywanie i udostępnianie **minimum 2^{100} obiektów**,

h) **Wydajność:**
   i) Rozwiązanie musi mieć architekturę zapewniającą wysoką wydajność jednoczesnego, równoległego, wielowątkowego składowania i dostępu do danych.
   ii) Zapis i odczyt pojedynczego obiektu musi osiągać **wydajność minimum 2GB/s**. Wydajność tą można uzyskać poprzez wykorzystanie wielu strumieni zapisu lub odczytu danych.
   iii) Zapis i odczyt wielu obiektów musi osiągać **wydajność co najmniej 1000 obiektów / sekundę.**
   iv) System musi zapewniać **obsługę co najmniej 100 000 równoległych żądań I/O** w stosunku do do przechowywanych obiektów i ich atrybutów a także kontenerów i ich atrybutów.

3. b. Wymagania szczegółowe dla macierzy obiektowych:

1) **Komponenty sprzętowe macierzy obiektowych:**
   a) **„Otwartość technologiczna" komponentów fizycznych macierzy:**
      i) węzły macierzy muszą być zbudowane przy wykorzystaniu standardowych komponentów sprzętowych dla serwerów, pamięci masowych i sieci dostępnych na otwartym rynku;
      ii) *nie dopuszcza się rozwiązań wykorzystujących dedykowane elementy sprzętowe dla uzyskania wydajności, pojemności i innych specjalizowanych funkcji takich jak np. układy ASIC produkowane wyłącznie przez producenta macierzy, których awaria wymuszałaby zakup specjalizowanego układu od tego producenta, po upływie gwarancji na zaoferowany system;*
      iii) *musi istnieć możliwość zakupu na otwartym rynku, po upływie okresu gwarancji i wsparcia dla systemu macierzy obiektowych elementów serwisowych dla węzłów systemu obiektowego, w tym napędów dyskowych, kontrolerów dyskowych a także dla elementów sieci komunikacyjnej*;
   b) **Architektura komponentów fizycznych macierzy:**
      i) Architektura komponentów fizycznych – węzłów macierzy (serwery, appliance) i elementów sieci LAN/SAN (jeśli taka sieć jest wymagana i jest częścią rozwiązania) – musi spełniać podstawowe wymagania związane z architekturą zdefiniowane dla komponentów serwerowych (systemu wysokiej dostępności, systemu baz danych) i sieciowych (sieci LAN/SAN), w szczególności:
         (1) Wszystkie elementy macierzy muszą być redundantne:
            (a) napędy dyskowe w węzłach (serwerach, appliance) macierzy obiektowej – muszą być redundantne i zapewniać możliwość realizacji nadmiarowego przechowywania danych oraz przejmowania obsługi żądań I/O w przypadku awarii pojedynczych komponentów;
            (b) Interfejsy i przełączniki sieci LAN/SAN (jeśli wymagane) – muszą zapewniać możliwość skonfigurowania redundantnych połączeń sieciowych w ramach macierzy obiektowej oraz pomiędzy klientami macierzy obiektowej a systemem macierzy obiektowych;
            (c) Zasilacze i wentylatory węzłów i przełączników – muszą zapewniać zasilanie i chłodzenie komponentów fizycznych macierzy pomimo awarii jednej z linii zasilania;
            (d) kontrolery dyskowe w węzłach (serwerach, appliance) macierzy obiektowej muszą zabezpieczać zawartość buforów do zapisu w przypadku nagłego zaniku zasilania;
   c) **Parametry minimalne komponentów sprzętowych macierzy:**
      i) **Napędy dyskowe:**
         (1) Dyski magnetyczne (HDD) dla danych:
            (a) Dopuszczalne technologie dysków magnetycznych (HDD): NL-SAS lub SATA;

(b) Możliwość wykorzystania dysków o pojemności 12TB, 14TB i 16TB.
(c) Dysk klasy enterprise: Minimalny MTBF [godzin]: 2 000 000

(2) Napędu flash (SSD/NVMe) dla meta-danych systemu obiektowego:
(a) Dopuszczalne technologie pamięci flash (SSD/NVMe): SAS, PCIe, M.2, SATA
(b) Dysk klasy enterprise: Minimalny MTBF [godzin]: 2 000 000
(c) Minimalna odporność na ścieranie [DWPD (ang. *disk writes per day*)]: 3

ii) **Interfejsy sieciowe**:
(1) Macierz obiektowa musi wykorzystywać do komunikacji standardowe interfejsy sieciowe, w technologii Ethernet o przepustowości 10Gbit lub wyższej, umożliwiające wykorzystanie minimum następujących funkcjonalności: dużych ramek (tzw. ang. *Jumbo Frames*), oraz agregację linków (z wykorzystaniem LACP), sieci wirtualne VLAN (802.1Q),.
(2) Macierz obiektowa musi być wyposażona w dedykowane interfejsy sieciowe do obsługi ruchu klienckiego oraz oddzielne, do obsługi redundantnego przechowywania i replikacji danych w macierzy – w celu zagwarantowania dedykowanej przepustowości ruchu produkcyjnego – do/z aplikacji, usług i narzędzi działających w systemie wysokiej dostępności;
(3) W przypadku, gdy dla uzyskania wymaganej wydajności w środowisku produkcyjnym (poza laboratorium), konieczne jest wykorzystanie wielu interfejsów sieciowych, macierz obiektowa musi być zaoferowana w konfiguracji zapewniającej agregację tych interfejsów, z uwzględnieniem cech i funkcji zaoferowanych przez Wykonawcę przełączników LAN sieci produkcyjnej dla infrastruktury serwerowej oraz zastosowanej w projekcie topologii tej sieci;

d) **Aspekty fizyczne komponentów macierzy obiektowej: obudowy, montaż, okablowanie:**
i) Macierz, tj. moduł kontrolera i obudowy pamięci/modułów pamięci flash (SSD/NVMe) oraz dysków magnetycznych (HDD) muszą być wyposażone w redundantne zasilacze i wentylatory. W każdym z modułów, redundantne zasilacze muszą mieć możliwość zasilania z różnych źródeł, bez potrzeby użycia zewnętrznych urządzeń.
ii) Elementy macierzy obiektowej muszą być montowalne w zaoferowanych przez Wykonawcę szafach przemysłowych 19”. Architektura rozwiązania musi być tak dobrana, by system w zaoferowanej pojemności (podstawowej i rozszerzonej – jeśli zaoferowano rozszerzenie) mógł być zainstalowany wraz z pozostałymi elementami infrastruktury serwerowej w 3 szafach rack w Centrum Podstawowym oraz 1 szafie rack w Centrum Zapasowym.
iii) Wraz z elementami sprzętowymi rozwiązania (węzły macierzy, elementy sieci) należy dostarczyć okablowanie zasilające i sieciowe, w tym dla sieci LAN i SAN (jeśli wymagane dla połączeń wewnętrznych); elementy sprzętowe macierzy obiektowej muszą być wyposażone w uchwyty umożliwiające ułożenie okablowania zgodnie z dobrymi praktykami; w szczególności dla okablowania optycznego należy dostarczyć prowadnice pozwalające na jego ułożenie z zachowaniem minimalnych promieni gięcia oraz eliminujące naprężenia okablowania podczas wykonywania czynności serwisowych takich jak wysuwanie serwerów czy wymiana dysków;

2) **Funkcjonalność:**
a) **Dostęp do danych –** protokoły dostępowe:
(1) Macierz musi realizować funkcjonalność funkcję obiektowego systemu przechowywania danych dostępnego dla “nowoczesnych aplikacji”, korzystających z protokołów takich jak S3, HTTP czy REST API.
(2) Macierz musi także zapewniać “zgodność wstecz” i dostępność dla aplikacji i narzędzi wykorzystujących klasyczne protokoły dostępowe do danych w tym plikowe, minimum NFS.
(3) W szczególności macierz obiektowa musi umożliwiać:
(a) składowanie danych oraz dostęp do danych i meta-danych poprzez protokół **Amazon S3**; *przy czym minimalny zakres wsparcia standardu S3 przez zaoferowaną macierz obiektową definiuje funkcjonalność infrastruktury serwerowej określona w punkcje „Opis koncepcyjny infrastruktury serwerowej” oraz opis funkcjonalności macierzy obiektowej;*
(b) prezentację i dostęp do danych i meta-danych przez **protokoły plikowe, minimum NFS** v3 a także – opcjonalnie – CIFS i SMB;
(c) **wielo-protokołowy dostęp** do tych samych zbiorów danych (obiektów, plików) zarówno poprzez protokoły obiektowe (minimum S3) jak i protokoły plikowe (minimum NFS);

b) **Składowanie danych:**
i) **Organizacja danych:**
(1) Macierze obiektowe muszą wspierać **wielopoziomowe zabezpieczenie fizyczne i logiczne danych** obejmujące lokalne składowanie nadmiarowe danych oraz replikację geograficzną;
(2) Macierz obiektowa musi umożliwiać **dynamiczną zmianę sposobu realizacji nadmiarowości** przechowywania lokalnego danych *on-line* (tj. w czasie normalnego użytkowania systemu, bez utraty dostępu dodanych), dla zapewnienia możliwości

dostosowania poziomu zabezpieczeń dla poszczególnych zbiorów danych lub kontenerów lub puli przechowywania danych macierzy;

(3) Macierze obiektowe muszą zapewniać **możliwość konfiguracji wielu obszarów logicznych** przechowywania danych (tzw. kontenery/ang. buckets/containers i pule/ang. vaults/tenants); dla tych obszarów logicznych musi być możliwa konfiguracja innych poziomów zabezpieczeń tj. redundancji przechowywania danych na poziomie lokalnym i geograficznym;

(4) Macierz obiektowa musi umożliwiać **dodawanie przestrzeni do przechowywania danych** bez przerywania pracy systemu – w szczególności dostęp do danych składowanych w systemie nie może być zaburzony (dane dostępne, brak degradacji wydajności) w czasie trwania procesu dodawania dodatkowej przestrzeni przechowywania danych;

(5) Po powiększeniu przestrzeni przechowywania danych w systemie – przez dodanie węzła systemu lub napędów dyskowych – macierz musi automatycznie realokować dane; taka funkcjonalność musi być realizowana *on-line*, bez konieczności migracji danych przechowywanych w macierzy lub ich przywracania z kopii zapasowych lub zdalnych replik;

ii) **Pojemność macierzy:** macierze obiektowe muszą zapewnić pojemność przechowywania danych:

(1) **Minimum 2200 TiB – pojemności logicznej**, tj. mierzonej po uwzględnieniu lokalnego przechowywania nadmiarowego oraz replikacji geograficznej pełnej zawartości macierzy; *przy czym pojemność ta musi być zrealizowana przy wykorzystaniu dostarczonych i skonfigurowanych w ramach macierzy obiektowej pamięci magnetycznych – dysków twardych (HDD) oraz pamięci flash (SSD/NVMe) – zapewniających natychmiastowy dostęp do danych; nie jest dopuszczalne wykorzystanie pamięci taśmowych z buforem dyskowym oraz technologii nearline, które powodowałyby opóźnienie dostępu do danych; nie jest dozwolone także dostarczanie pojemności uzyskanej na bazie zewnętrznych systemów przechowywania danych, typu usługi chmurowe czy inne zasoby pozyskane przez Wykonawcę poprzez outsourcing;*

(2) **Zaoferowanie pojemność logicznej powyżej 2200 TiB będzie dodatkowo punktowane** – zgodnie z opisem kryterium technicznego „O"; (poj. logiczna – zgodnie z powyższą definicją);

(3) Minimum **5%** pojemności logicznej macierzy obiektowej – musi być zrealizowane przy wykorzystaniu pamięci flash (SSD/NVMe) – dla zapewnienia wydajnej przestrzeni dla meta-danych systemu obiektowego i meta-danych poziomu użytkownika oraz buforowania danych;

iii) **Redundancja danych**:

(1) macierz obiektowa musi wspierać elastyczne konfigurowanie poziomu przechowywania nadmiarowego danych (tzw. ang. *Erasure Coding*), w tym możliwość wskazywania poziomu odporności macierzy obiektowej na awarię określonej liczby komponentów w tym: węzłów (serwerów, appliance) macierzy obiektowej i/lub napędów dyskowych (HDD);

(2) założony przez Wykonawcę dla określenia pojemności logicznej macierzy poziom redundancji danych musi być wskazany w ofercie (formularz i kalkulacja pojemności logicznej macierzy);

iv) **Replikacja geograficzna**:

(1) wymagane jest zapewnienie **replikacji geograficznej** przechowywanych lokalnie danych;

(2) replikacja geograficzna musi być wspierana minimum w trybie: **asynchronicznym**;

v) **Elastyczność konfiguracji** zabezpieczenia danych; **buforowanie** danych:

(1) macierz obiektowa musi wspierać możliwość różnicowania poziomu ochrony danych, w tym przechowywania nadmiarowego danych (tzw. ang. *Erasure Coding*) lub replikacji danych dla różnych typów mediów/pamięci, kontenerów i użytkowników/grup – minimum musi być możliwe skonfigurowanie kodowania nadmiarowego dla danych przechowywanych na pamięciach magnetycznych – dyski twarde (HDD) oraz replikacji dla danych lub meta-danych przechowywanych na pamięciach flash (SSD/NVMe) a także musi istnieć możliwość wyróżnienia obszarów/zbiorów danych przechowywanych wyłącznie lokalnie (tylko kodowanie nadmiarowe w ramach centrum danych) oraz w trybie replikacji geograficznej (kodowanie nadmiarowe w ramach centrum danych plus replikacja między centrami danych);

(2) macierz obiektowa musi umożliwiać dynamiczne buforowanie danych przechowywanych na dyskach magnetycznych (HDD) – z wykorzystaniem szybszych pamięci flash (SSD/NVMe);

c) **Funkcjonalność zaawansowana:**

i) Zabezpieczenie składowanych obiektów w systemie:

(1) **Replikacja danych a wysoka dostępność systemu macierzy dyskowych:**

(a) Wymagane jest wsparcie dla zabezpieczenia integralności i dostępności danych poprzez zdefiniowaną replikację geograficzną (asynchroniczną lub synchroniczną) pomiędzy odrębnymi macierzami obiektowymi umożliwiające przełączanie i przejmowanie obsługi żądań dostępu do danych i składowania danych w trybie *active-active* lub *active-passive*;

(b) *Nie jest wymagana realizacja replikacji synchronicznej oraz pracy w trybie active-active, dopuszczalne jest realizacja replikacji danych w macierzy w modelu tzw. eventual*

consistency; jednocześnie tolerowane są chwilowe niespójności danych pomiędzy dwoma macierzami obiektowymi, wynikające z realizacji replikacji w modelu asynchronicznym;

(2) **Funkcjonalność typu WORM:**
   (a) Wymagane jest wsparcie funkcjonalności zabezpieczenia danych w macierzach obiektowych przed usunięciem, modyfikacją, utratą integralności, wskutek błędu lub awarii systemu, błędu użytkownika czy celowego działania lub ataku (np. *ransomware*). W szczególności macierz musi umożliwiać:
      (i) blokowanie możliwości zapisania/nadpisania danych – funkcjonalność typu WORM,
      (ii) zastrzeżenie/ograniczenie możliwości skasowania danych lub wyłączenia mechanizmu WORM dla danych przed upływem określonego czasu (okna retencji);
   (b) Nie jest wymagane zapewnienia funkcjonalności i cech „trwałego nośnika" zgodnie z definicją tego pojęcia w polskich aktach prawnych oraz przedstawioną przez UOKiK.

(3) **Retencja obiektów:**
   (a) Wymagane jest wsparcie dla tworzenie różnych polityk retencji obiektów (np. planowane zarządzanie ilością kopii, ich rozmieszczenie w obrębie systemu, automatyczne kasowanie obiektów) dla różnych puli danych; polityki retencji muszą być implementowane przez oprogramowanie macierzy obiektowej a ich wykonanie raportowane dla administratora;
   (b) Wymagana jest realizacja automatyczna polityk retencji danych, przy czym: dopuszczalna jest realizacja asynchroniczna polityk retencji danych z niewielkim opóźnienie w stosunku do składowania czy modyfikacji danych; *nie jest wymagane realizowanie polityk retencji danych w trybie on-line (natychmiastowo po składowaniu / modyfikacji danych);*
   (c) Wymagana jest realizacja mechanizmu zmiany schematów protekcji obiektów*; przy czym funkcjonalność ta musi być realizowana minimum w odpowiedzi na żądanie użytkownika lub administratora przez interfejs zarządzania macierzy obiektowej bądź w reakcji wywołanie funkcjonalności macierzy obiektowych przez odpowiednie CLI/API macierzy; nie jest wymagana realizacja automatycznej zmiany schematów protekcji obiektów całkowicie automatycznie w oparciu o ich czas stworzenia, modyfikacji, czy dostępu;*

(4) **Wersjonowanie danych:**
   (a) Wymagane jest wsparcie funkcjonalności wersjonowanie danych
   (b) W szczególności macierz musi umożliwiać:
      (i) automatyczne tworzenie wersji obiektów – po nadpisaniu obiektu istniejącego w macierzy obiektowej nową wersją obiektu lub modyfikacji fragmentu obiektu
      (ii) prezentację i dostęp użytkownika do wielu wersji oraz zarządzanie wersjami (usuwanie wersji, wskazanie aktualnej wersji, wycofanie zmian obiektu);
      (iii) możliwość „przywrócenia" to jest wskazania historycznych wersji jako aktualnych, domyślnie prezentowanych i dostępnych wersji obiektów z poziomu interfejsu zarządzania macierzą obiektową lub *przez odpowiednie CLI/API macierzy;*

(5) **Obsługa meta-danych:**
   (a) Wymagane jest wsparcie funkcjonalności definiowania zaawansowanych meta-danych (poziomu użytkownika w przeciwieństwie do meta-danych systemowych) zarówno dla obiektów jak i kontenerów składowanych w systemie przechowywania obiektowego;
   (b) Konieczne jest wsparcie możliwości przeszukiwania meta-danych przechowywanych obiektów oraz meta-danych kontenerów; wyszukiwanie meta-danych musi być możliwe;
      (i) poprzez interfejs programistyczny, tj. odpowiednią funkcję REST API (standard S3);
      (ii) za pomocą interfejsu graficznego użytkownika archiwum systemu obiektowego– poprzez narzędzie/formularz do przeszukiwania meta-danych poziomu użytkownika;
   (c) Zaoferowane rozwiązanie – system macierzy obiektowych wraz z narzędziami – zintegrowanymi i gotowymi do użycia przez użytkownika i administratora oraz aplikacje i usługi działające na systemie wysokiej dostępności, korzystające z macierzy poprzez API i protokoły S3 – musi wspierać indeksację meta-danych w celu przyśpieszenia wyszukiwania meta-danych (bez konieczności skanowania całego zbioru danych czy meta-danych w odpowiedzi na zapytanie / żądanie przeszukiwania meta-danych);
   (d) Macierz obiektowa musi umożliwiać składowanie meta-danych poziomu użytkownika na szybkich pamięciach flash (SSD/NVMe) lub ich buforowania w pamięci RAM węzłów (serwerów, appliance) macierz obiektowej lub na pamięciach flash (SSD/NVMe) lub realizować inny mechanizm zapewniający wydajny dostęp i wyszukiwanie meta-danych;

(6) **Redukcja danych**:
   (a) Macierz obiektowa musi wspierać funkcjonalność redukcji danych w systemie przechowywania danych poprzez **kompresję danych lub deduplikację danych**;

(b) Funkcjonalność redukcji danych wymieniona w ppkt. a) musi być realizowana mechanizmami wewnętrznymi macierzy obiektowej; funkcjonalność ta *może być realizowana asynchronicznie w stosunku do składowania danych; przykładowo dane mogą być deduplikowane z opóźnieniem w stosunku do składowania ich w systemie za pomocą procesów działających asynchronicznie, w tle w stosunku do procesów obsługi I/O w systemie obiektowym, jednakże procesy te muszą być zintegrowane w macierzy obiektowej i kontrolowane przez oprogramowanie macierzy obiektowej;*

(c) *Uwaga! Wymagana pojemność logiczna macierzy musi być wyliczona bez uwzględniania kompresji i deduplikacji danych z uwagi na nieznaną a priori skuteczność tych mechanizmów dla danych archiwalnych obiektów cyfrowych Biblioteki Śląskiej*

3) **Niezawodność:**
   a) Mechanizmy wysokiej dostępności:
      i) **Odbudowa struktur przechowywania danych**:
         (1) Macierz obiektowa musi realizować automatycznie odbudowę struktur przechowywania danych, w celu przywrócenia zadanej nadmiarowości przechowywania danych po awarii węzła systemu (serwera, appliance) lub napędów dyskowych w ramach węzłów systemu;
         (2) automatyczny proces odbudowy nie może powodować niedostępności danych ani *degradacji wydajności macierzy obiektowej (powodującej przeterminowanie żądań I/O) z punktu widzenia użytkownika w tym aplikacji, narzędzi i usług działających na systemie wysokiej dostępności;*
      ii) System macierzy obiektowych musi umożliwiać **przełączenie obsługi żądań I/O** (składowanie i dostęp do danych, operacje na meta-danych, listowanie kontenerów i atrybutów obiektów):
         (1) pomiędzy węzłami macierzy w ramach centrum danych – w przypadku awarii określonej, dopuszczalnej liczby węzłów lub dysków macierzy obiektowej w ramach centrum danych
         (2) pomiędzy centrami danych – w przypadku awarii w jednym z centrów danych przekraczającej liczbę węzłów lub dysków pozwalającą na działanie macierzy w tym centrum danych;
      iii) System musi umożliwiać **wykonanie operacji serwisowych w sposób nie przerywający pracy** macierzy obiektowej; w czasie tych operacji musi być możliwe składowanie i dostęp do danych w sposób niezaburzony z punktu widzenia dostępności usług składowania i pobierania danych, dostępności danych oraz wydajności składowania i dostępu do danych; wymóg ten dotyczy:
         (1) wymiany pojedynczych komponentów macierzy (dysków, kontrolerów, zasilaczy etc.);
         (2) wymiany/dodawania węzłów (serwer, appliance) macierzy obiektowej;
         (3) aktualizacji oprogramowania macierzy (warstwa oprogramowania systemu obiektowego);
         (4) aktualizacji systemów operacyjnych i/lub mikrokodu (firmware) elementów sprzętowych;
      iv) **Proaktywny monitoring, przewidywanie awarii**, przeciwdziałanie skutkom awarii:
         (1) System musi wykrywać potencjalnie zbliżającą się awarię dysków oraz proaktwnie przenosić dane znajdujące się na zagrożonych awarią dyskach na inne dyski niezagrożone awarią;
         (2) W ramach implementacji powyższej funkcjonalności macierz obiektowa musi zapewiać minimum, że kontrolery dyskowe w węzłach (serwerach, appliance) macierzy obiektowej proaktywnie monitorują stan dysków magnetycznych (HDD) i pamięci flash (SSD/NVMe) w celu wykrywania prawdopodobieństwa ich awarii – minimum na podstawie analizy danych z systemu SMART oraz informacji o zużyciu (ang. *wear*) pamięci flash (SSD/NVMe);
         (3) Węzły macierzy obiektowej (serwery, appliance) – muszą wpierać automatyczne wyłączanie w odpowiedzi na zgłoszoną przez system UPS awarię zasilania sieciowego;
4) **Bezpieczeństwo:**
   a) **Uwierzytelnianie i autoryzacja** użytkowników:
      i) system musi umożliwiać **uwierzytelnianie** (autentykację) użytkowników na bazie minimum:
         (1) tzw. user key i secret access key – zgodnie ze standardem S3
         (2) Loginu i hasła użytkownika
         (3) Konta użytkownika w usłudze katalogowej (wsparcie dla minimum Active Directory i LDAP);
      ii) System musi **autoryzować** użytkowników i umożliwiać kontrolę dostępu na bazie:
         (1) Nazw/identyfikatorów użytkowników i ich przynależności do grup
         (2) Ról użytkowników i grupy użytkowników (tzw. role-based access control / RBAC)
   b) **Ochrona kryptograficzna** danych i komunikacji i zarządzanie kluczami – system musi zapewniać
      i) szyfrowanie przechowywanych danych minimum algorytmem AES-256.
      ii) szyfrowanie transmisji danych minimum protokołem TLS 1.2.
      iii) zarządzanie wewnętrznymi kluczami szyfrującymi;
5) **Zarządzanie macierzami obiektowymi:**
   a) System musi monitorować stan macierzy obiektowej i jej komponentów i stan procesów zarządzania danymi w ramach każdej macierzy obiektowej i połączonego systemu macierzy dyskowych – w tym:

i) Monitorować (i prezentować w interfejsie zarządzania) kluczowe parametry stanu macierzy obiektowych w tym: pojemność i dostępność przestrzeni w pulach dyskowych, objętość zbiorów danych w kontenerach i pulach przepustowość/wydajność operacji składowania i dostępu do danych, obciążenie elementów macierzy obiektowej obsługą ruchu (np. użycie dysków w MB/s, ilość obsługiwanych operacji I/O w jednostce czasu - IOPS), obciążenie procesorów i wykorzystanie pamięci RAM w węzłach (serwerach/appliance) macierzy;
ii) Prezentować dane monitoringowe w graficznym panelu informacyjnym (tzw. ang. dashboard) dostępnym poprzez interfejs Web do zarządzania/monitoringu macierzy obiektowej lub poprzez dedykowaną aplikację do zarządzania macierzą obiektową dostępną co najmniej dla środowiska Windows 10 oraz współczesnych dystrybucji systemów Linuxowych (RHEL, SLES, Ubuntu);
iii) Wspierać protokół Simple Network Management Protocol (SNMP) v3;
iv) Wykrywać awarie komponentów sprzętowych lub przekroczenie wartości progowych zdefiniowanych dla parametrów pracy macierzy obiektowej oraz monitować administratora o wystąpieniu awarii lub przekroczeniu wartości progowych (email, trapy protokołu SNMP);
v) Wykrywać anomalie dot. pracy macierzy w tym spowolnienie obsługi żądań I/O wskutek awarii sprzętowych lub programowych lub przeciążenia systemu procesami obsługi I/O oraz odbudowy redundancji danych po awarii lub rekonfiguracji macierzy (np. dodanie dysków czy węzłów);
vi) Umożliwiać tworzenie zagregowanych, historycznych raportów i podsumowań dotyczących obciążenia elementów macierzy obiektowej, wolumenu ruchu I/O do/z macierzy obiektowej (pasmo, liczba operacji I/O), wykorzystania powierzchni przechowywania danych, liczby obiektów przechowywanych w macierzy, wydajności/niezawodności procesu replikacji geograficznej;

b) *Uwaga! funkcjonalność monitorowania i zarządzania macierzą musi być integralną, utrzymywaną i rozwijaną częścią zaoferowanego produktu – macierzy obiektowej; w szczególności funkcjonalność ta nie może być stworzona i zaoferowana wyłącznie na potrzeby niniejszego projektu/zamówien*ia;

6) **„Otwartość technologiczna" archiwum obiektowego:**
a) Protokoły dostępowe macierzy obiektowej, mechanizmy wewnętrzne macierzy oraz zastosowane i dostarczone przez Wykonawcę funkcje i licencje muszą umożliwiać masową migrację danych (wolumen rzędu kilkuset TiB), zarówno do macierzy obiektowej (migracja danych z istniejących systemów przechowywania danych) jak i masową migrację danych (rzędu 2-3PB) na zewnątrz macierzy obiektowej (potencjalna migracja danych w przyszłości na inne systemy przechowywania danych); w szczególności wyniesienie wszystkich danych składowanych w macierzy obiektowej poza tę macierz nie może wiązać się z ponoszeniem przez użytkownika / instytucję żadnych dodatkowych kosztów licencji czy zakupu funkcjonalności zarówno podczas jak i po zakończeniu okresu licencji, subskrypcji lub wsparcia serwisowego zaoferowanych w ramach realizacji niniejszego zamówienia;
b) System macierzy obiektowych musi – z punktu widzenia architektury i technologii sprzętowych oraz wbudowanych w system mechanizmów zarządzania danymi – zapewniać możliwość wycofywania z użycia w zaoferowanej infrastrukturze macierzy obiektowych starszych komponentów w tym modeli węzłów (serwerów, appliance), napędów dyskowych oraz innych elementów rozwiązania (np. sieć) oraz zastępowania ich nowszymi komponentami – w tym nowszymi modelami węzłów (serwerów, appliance) pochodzącymi od producenta rozwiązania czy nowszymi modelami napędów dyskowych (pochodzących z otwartej dystrybucji lub od producenta zaoferowanego rozwiązania); stopniowa migracja danych na nowocześniejsze komponenty w tym węzły (serwery, appliance) i napędy dyskowe nie może wymagać przerwy w działaniu macierzy obiektowej, w szczególności nie może powodować utraty możliwości składowania i dostępu do danych przechowywanych w systemie;

7) Dojrzałość produktu: Zaoferowany system macierzy obiektowych musi być produktem obecnym na rynku IT **od co najmniej 3 lat** oraz stanowić kompletne rozwiązanie sprzętowo-programowe, w szczególności:
i) Producent macierzy obiektowej musi być odnotowywany w zestawieniach i raportach uznanych organizacji działających w sektorze usług i systemów IT, w tym minimum: w raportach firmy Gartner za lata 2018, 2019 i 2020; dla roku 2020 należy odnosić się do raportu „Magic Quadrant for Distributed File Systems and Object" (adres dostępowy do dokumentu: https://www.gartner.com/en/documents/3991764);
ii) Uwaga! Wymóg ten dotyczy oprogramowania macierzy obiektowej; dopuszczalne jest zaoferowanie macierzy obiektowych w oparciu o nowe modele węzłów (serwery, appliance), niespełniające wymogu dostępności od 3 lat na rynku, jednakże zgodne z oprogramowaniem systemu obiektowego, tj. znajdujące się na liście kompatybilności tego oprogramowania;
b) Zaoferowany system musi być produktem gotowym, posiadającym na moment składania oferty wszystkie wymagane przez Zamawiającego funkcjonalność, opisane w powszechnie dostępnej dokumentacji rozwiązania (specyfikacje, katalogi, dokumentacja techniczna, tzw. white-paper);

4. SIEĆ LAN i SYSTEM UTM ORAZ SIEĆ SAN

Infrastruktura sieciowa dostarczana w ramach zamówienia obejmuje sieć LAN i system UTM oraz sieć SAN dla infrastruktury serwerowej łączące elementy dostarczonej infrastruktury serwerowej (system wysokiej dostępności, systemu baz danych NoSQL, elementy macierzy centralnej, macierze obiektowe, system wykonywania kopii zapasowych) z siecią LAN i łączami WAN Biblioteki Śląskiej.

Ponadto, dostarczane w ramach zamówienia elementy sieci LAN obejmują przełączniki dla pracowni digitalizacyjnej i czytelni Biblioteki Śląskiej umożliwiające podłączenie stacji roboczych zlokalizowanych w pomieszczeniach pracowni do sieci LAN dla infrastruktury serwerowej, zapewniając odpowiednią wydajność dostępu do usług infrastruktury serwerowej z poziomu pracowni Biblioteki Śląskiej.

4.a. Sieć LAN dla infrastruktury serwerowej

Sieć LAN dla infrastruktury serwerowej obejmuje:

- **sieć produkcyjną LAN** – zbudowaną w oparciu o przełączniki 10/40 (lub 25/100) Gbit Ethernet, za pomocą której stworzone zostaną połączenia wewnętrzne w ramach dostarczanej infrastruktury serwerowej oraz połączenia zewnętrzne, to jest połączenia z siecią LAN istniejącej infrastruktury IT Biblioteki Śląskiej:
  - połączenia systemu wysokiej dostępności z serwerami systemu baz danych NoSQL oraz elementami macierzy centralnej (dyskowej) realizującymi usługi plikowe NFS, CIFS a także z systemem wykonywania kopii zapasowych);
  - połączenia systemu wysokiej dostępności oraz systemu baz danych NoSQL z siecią wewnętrzną LAN w ramach Biblioteki Śląskiej oraz poprzez sieć LAN z siecią Internet poprzez łącza WAN
  - połączenia pomiędzy elementami macierzy zlokalizowanymi w Centrum Podstawowym i Centrum Zapasowym Biblioteki Śląskiej – na potrzeby replikacji danych w ramach macierzy obiektowej;
  - połączenia między elementami systemu wykonywania kopii zapasowych zlokalizowanymi w Centrum Podstawowym i Centrum Zapasowym Biblioteki Śląskiej – m.in. na potrzeby replikacji danych w ramach systemu wykonywania kopii zapasowych oraz efektywnego odtwarzania danych w przypadki rozległej awarii w Centrum Podstawowym;
  - połączenia dostarczanej infrastruktury sieciowej LAN z istniejącą siecią LAN istniejącej infrastruktury IT Biblioteki Śląskiej obejmującej serwery, systemy przechowywania danych, przyłącza do Internetu, pracownie digitalizacyjne i czytelnie cyfrowe;
- **sieć do zarządzania LAN** – zbudowaną w oparciu o przełączniki 1/10 Gbit Ethernet, za pomocą której stworzone zostaną połączenia wewnętrzne w ramach infrastruktury serwerowej na potrzeby zarządzania infrastrukturą serwerową oraz budowy sieci wewnętrznej zarządzającej środowisk wirtualnych w tym:
  - zarządzanie serwerami fizycznymi systemu wysokiej dostępności i systemu baz danych NoSQL
  - zarządzanie macierzą centralną (dyskową) oraz macierzą obiektową
  - zarządzanie systemem wykonywania kopii zapasowych;
  - sieci wewnętrznej zarządzającej środowisk wirtualnych (na potrzeby zarządzania, monitoringu, tzw. *hearbeat*, synchronizacji danych o stanie środowiska, realizacji procesów migracji maszyn wirtualnych między serwerami, dostępu do konsoli zarządzającej platformy wirtualizacyjnej);
  - sieci wewnętrznej środowiska systemu baz danych NoSQL wirtualnych (na potrzeby zarządzania klastrem baz danych, monitoringu, tzw. *heartbeat*, synchronizacji danych o stanie klastra, itp.);
- **system UTM** – zapewniający ochronę zewnętrznego i wewnętrznego ruchu sieciowego w ramach dostarczanej infrastruktury serwerowej Biblioteki Śląskiej (oraz istniejącej infrastruktury)

Elementy sieci LAN dla infrastruktury serwerowej muszą spełniać co najmniej poniższe wymagania dotyczące cech i funkcjonalności przełączników sieciowych, topologii sieci oraz funkcjonalności systemu ochrony ruchu sieciowego – przy czym wszystkie wymagania muszą być traktowane jako minimalne, chyba że treść wymogu stanowi inaczej.

4.a.1 Przełączniki sieci LAN dla infrastruktury serwerowej

Przełączniki sieci LAN obejmują przełączniki w technologii Gigabit Ethernet dla sieci LAN produkcyjnej o przepustowości 10/40 (25/100) Gbit/s i przełączniki dla sieci LAN do zarządzania o przepustowości 1/10 Gbit/s.

1. Wymagania ogólne dla sieci LAN dla infrastruktury serwerowej:

a) Wymagana jest dostawa takiej liczby przełączników sieci LAN, która umożliwia realizację wymaganej topologii połączeń w sieci LAN, przy czym należy dostarczyć nie mniej niż:
   i) 6 przełączników sieci LAN produkcyjnej 10/40 (25/100) Gigabit Ethernet
   ii) 4 przełączników sieci LAN do zarządzania 1/10 Gigabit Ethernet

2. Topologia sieci LAN dla infrastruktury serwerowej:

a) Topologia wymaganych połączeń w sieci LAN produkcyjnej:

i) Przełączniki sieci produkcyjnej LAN muszą zapewniać niezawodne połączenia do serwerów systemu wysokiej dostępności oraz systemu baz danych noSQL z wykorzystaniem redundantnych portów sieci produkcyjnej LAN w dostarczanych serwerach.

ii) Zastosowane przełączniki (liczba, typ, przepustowość, liczba portów) oraz topologia połączeń muszą umożliwiać pracę portów serwerów z pełną przepustowością umożliwiającą strumieniową transmisję przez te porty danych pomiędzy dowolną parą serwerów systemu wysokiej dostępności oraz systemu baz danych NoSQL z wydajnością minimum 0,8GB/s (Gigabajta) na sekundę per serwer (w jednym kierunku);

iii) Po wykonaniu wymaganych połączeń w każdym przełączniku LAN sieci produkcyjnej musi pozostać **rezerwa minimum 25% portów** (od strony serwerów i urządzeń, nie dotyczy tzw. uplinków); porty te muszą być obsadzone wkładkami (identycznymi jak porty do serwerów i urządzeń) oraz aktywowane;

b) Topologia wymaganych połączeń w sieci LAN do zarządzania:

i) Przełączniki sieci LAN do zarządzania muszą zapewniać minimum pojedyncze połączenia do dedykowanych portów do zarządzania w serwerach systemu wysokiej dostępności i serwerów systemu baz danych (dla konsoli systemu i zarządzania przez IPMI) oraz portów dostępowych konsoli/urządzenia KVM a także portów do zarządzania macierzy centralnej (dyskowej), macierzy obiektowej i elementów systemu wykonywania kopii zapasowych a także portów do zarządzania elementami infrastruktury sieciowej (przełączniki LAN, SAN i system UTM);

ii) Po wykonaniu wymaganych połączeń w przełącznikach LAN sieci do zarządzania musi pozostać **rezerwa sumarycznie minimum 25% liczby portów** (od strony serwerów i urządzeń, nie dotyczy tzw. uplinków); porty te muszą być obsadzone wkładkami (jeśli wymagane) oraz aktywowane;

3. Wymagania dla przełączników sieci LAN dla infrastruktury serwerowej:

a) **Wymagania dla każdego z przełączników sieci LAN produkcyjnej** (10/40Gbit lub 25/100Gbit):

i) porty do podłączania serwerów – wymagania minimalne:
   (1) liczba portów do podłączania serwerów: **48**
   (2) przepustowość każdego z portów do podłączania serwerów 10Gbit lub wyższa (np. 25Gbit)

ii) porty uplink – do przełączników agregujących – wymagania minimalne:
   (1) liczba uplinków przypadających na każde 48 portów do serwerów: **4**
   (2) przepustowość każdego z portów uplink min. 40Gbit/s lub wyższa (np. 100Gbit)

iii) warianty realizacji wymaganej liczby portów:
   (1) preferowana przez Zamawiającego jest realizacja wymaganej liczby portów przełączników do podłączania serwerów poprzez zaoferowanie przełączników posiadających w obudowie przełącznika wymaganą liczbę portów (bez stosowania kabli rozszywających linki wyższej prędkości na linki niższej prędkości)
   (2) dozwolone jest jednak także zrealizowanie wymaganej liczby portów przełączników do serwerów poprzez zastosowanie rozwiązań, w których porty 40GBit Ethernet lub 100Gbit Ethernet przełącznika są rozszywane odpowiednio na 4 porty 10Gbit Ethernet lub na 4 porty 25 Gbit Ethernet, a tak rozdzielone kanały są wykorzystywane do podłączania serwerów;

iv) Funkcjonalność przełączników:
   (1) wsparcie dla minimum 4000 VLAN, kompatybilność z 802.1Q
   (2) wsparcie dla Jumbo Frames
   (3) wsparcie dla LLDP, MSTP, LACP, SNMP
   (4) wsparcie dla agregacji połączeń zgodnie z 802.3AD
   (1) tablica MAC min. 200 000 wpisów
   (2) Wielkość bufora wewnętrznego przełącznika: co najmniej 12MB.
   (3) zarządzanie przez SSH; wsparcie dla zarządzania i monitorowania przełącznika out-of-band za pomocą dedykowanych interfejsów/portów podłączonych do sieci LAN do zarządzania.
   (4) wsparcie dla OpenFlow1.3 lub innych technologii SDN (ang. Software Defined Network)

ii) Architektura logiczna / wydajność:
   (1) Przełącznik musi posiadać architekturę non-blocking.
   (2) Opóźnienie wprowadzane przez przełącznik nie może być większe niż 0.8 mikrosekundy,
   (3) Przepustowość magistral wewnętrznych przełącznika: co najmniej **2 Tbps**.
   (4) Wydajność przełączania: **100 mln pakietów**
   (5) Wsparcie dla łączenia przełączników w stos (do 10 przełączników)

i) Wszystkie wolne porty przełączników do serwerów muszą być aktywowane (mieć dostarczoną licencję) oraz być wyposażone we wkładki optyczne SFP+ SR MM oraz posiadać licencje pozwalające na realizację zdefiniowanej powyższymi wymaganiami funkcjonalności przełącznika;

ii) Wszystkie porty uplink muszą być aktywowane i wyposażone we wkładki oraz posiadać licencje pozwalające na realizację zdefiniowanej powyższymi wymaganiami funkcjonalności przełącznika;

b) **Wymagania dla każdego z przełączników sieci LAN do zarządzania 1/10 Gbit:**
   i) porty do podłączania urządzeń zarządzanych przez sieć LAN – wymagania minimalne:
      (1) liczba portów do podłączania urządzeń zarządzanych przez sieć LAN urządzeń : **48**
      (2) przepustowość każdego z portów 1Gbit lub wyższa (np. 25Gbit)
   ii) porty uplink – do przełączników agregujących – wymagania minimalne:
      (1) liczba uplinków przypadających na każde 48 portów do serwerów: **2**
      (2) przepustowość każdego z portów uplink min. 10Gbit/s lub wyższa (np. 25Gbit/s)
   iii) Funkcjonalność przełączników:
      (1) wsparcie technologii dla minimum 4000 VLAN, kompatybilny z 802.1Q;
      (2) wsparcie technologii dla Jumbo Frames;
      (3) wsparcie tablicy MAC min. 20 000 wpisów;
      (4) zarządzanie przez SSH; wsparcie dla zarządzania i monitorowania przełącznika out-of-band za pomocą dedykowanych interfejsów/portów podłączonych do sieci LAN do zarządzania;
   iv) Architektura logiczna / wydajność:
      (1) Przepustowość magistral wewnętrznych przełącznika: co najmniej **2 Tbit/s**
      (2) Wydajność przełączania: **100 mln pakietów**
      (3) Wsparcie dla łączenia przełączników w stos (do 10 przełączników)
   v) po wykonaniu połączeń do zarządzanych przez przełączniki VLAN do zarządzania elementów infrastruktury, w każdym przełączniku do zarządzania musi pozostać minimum 25% wolnych portów o przepustowości co najmniej 1 Gbit/s

c) **Wymagania wspólne dla przełączników sieci LAN dla infrastruktury serwerowej:**
   i) Architektura fizyczna przełączników
      (1) Przełączniki być muszą być rackowalne,
      (2) Przełącznik musi mieć wysokość maksymalną 1U na każde 48-portów 10 lub 25Gbit do serwerów lub urządzeń zarządzanych przez sieć LAN
      (3) zakłada się możliwość instalacji przełączników zarówno od frontu jak od tyłu serwerów – decyzja projektowa musi być podjęta przez Wykonawcę i musi być podyktowana dążeniem do minimalizacji stopnia skomplikowania okablowania; należy przy tym dostosować kierunek przepływu powietrza przez przełącznik do planowanej orientacji przełącznika w szafie;
      (4) Przełącznik musi być zasilany z co najmniej dwóch redundantnych zasilaczy, które mogą być zasilane z dwóch niezależnych źródeł zasilania oraz mogą być wymieniane na gorąco.
   ii) Przełączniki muszą być dostarczone wraz z elementami niezbędnymi do ich poprawnej instalacji w szafach dostarczanych przez Wykonawcę, w ustalonej przez Wykonawcę lokalizacji w szafach oraz orientacji w stosunku do kierunku przepływu powietrza przez serwery i inne elementy infrastruktury serwerowej (macierze, appliance etc.).
   iii) Dla przełączników sieciowych LAN muszą być dostarczone organizatory okablowania wyposażone w uchwyty umożliwiające ułożenie okablowania zgodnie z dobrymi praktykami; w szczególności dla okablowania optycznego muszą zostać być dostarczone prowadnice pozwalające na ułożenie okablowania optycznego z zachowaniem minimalnych promieni gięcia oraz eliminujące naprężenia okablowania podczas wykonywania czynności serwisowych;

4.a.2 Urządzenie UTM

Urządzenie UTM zapewniać będzie ochronę zewnętrznego i wewnętrznego ruchu sieciowego w sieci LAN w ramach dostarczanej infrastruktury serwerowej Biblioteki Śląskiej (a także istniejącej infrastruktury).

1. Wymagania ogólne

a) Architektura:
   i) Klaster zapór sieciowych dostarczony w postaci zestawu dwóch fizycznych, niezależnych, identycznych urządzeń sieciowych UTM (2 sztuki) wraz z zainstalowanym oprogramowaniem, pochodzących od jednego producenta.
   ii) System musi być zrealizowany jako tzw. *appliance* to jest rozwiązanie będące połączeniem sprzętu i oprogramowania tego samego producenta, oferowane jako zintegrowane rozwiązanie występujące w ofercie / katalogu producenta oraz jego cenniku.

b) Podzespoły – urządzenie musi posiadać minimum:
   i) pamięć DRAM o pojemności nie mniejszej niż 8 GB pozwalająca jednocześnie na zrealizowanie wszystkich wymagań zdefiniowanych w opisie przedmiotu zamówienia,
   ii) dysk HDD o pojemności nie mniejszej niż 320GB,

iii) 2 redundantne zasilacze umożliwiające zasilanie prądem przemiennym 230V (niedopuszczalne rozwiązania zewnętrzne) z możliwością wymiany w trakcie pracy urządzenia (ang. hot- swap).

c) Aspekty fizyczne
   i) Urządzenie musi posiadać wysokość nie więcej niż 1U,
   ii) Każde z dostarczonych dwóch urządzeń musi być przystosowane do zamontowania w szafie rack 19" i ma zostać dostarczone wraz z niezbędnym do montażu sprzętem i okablowaniem oraz licencją na zewnętrzny centralny system zarządzania. Przez „Urządzenie" rozumiemy każde z pary zaoferowanych urządzeń.

2. Funkcjonalność

a) **Firewall**:
   i) Urządzenie musi realizować inspekcję stanową opartą na granularnej analizie komunikacji oraz stanu aplikacji w celu poprawnego śledzenia i kontroli przepływu ruchu.
   ii) Urządzenie musi posiadać przepustowość firewalla nie mniejszą niż 31 Gbps dla pakietów UDP 1518B mierzoną w warunkach laboratoryjnych.
   iii) Urządzenie musi posiadać możliwość zaraportowania ilości „trafień" wybranej polityki do aplikacji zarządzającej.
   iv) Tworzenie reguł musi pozwalać na ich konfiguracje w określonych interwałach czasowych wraz z podaniem daty lub godziny ich wygaśnięcia.
   v) Urządzenie musi posiadać możliwość konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika (Identity Firewall), integrując się ściśle z usługą katalogową Microsoft Active Directory.
   vi) Klaster musi posiadać możliwość skorzystania z lokalnej bazy użytkowników pozwalając na ich autentykację bez potrzeby korzystania z zewnętrznych rozwiązań.
   vii) Urządzenie pracujące w klastrze musi umożliwiać pracę w trybie Transparent/Bridge.
   viii) Rozwiązanie musi wspierać wysoką dostępność (HA) Active/Active oraz Active/Passive wraz z dzieleniem obciążenia i synchronizacją stanu. Urządzenia pracujące w klastrze muszą synchronizować co najmniej tablice stanów oraz konfigurację. Klaster musi posiadać możliwość aktualizacji oprogramowania urządzeń wchodzących w skład klastra w taki sposób, aby w trakcie aktualizacji nie doszło do przerwania obsługi ruchu sieciowego. .
   ix) Urządzenie nie powinno mieć ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej.
   x) Rozwiązanie musi posiadać możliwość komunikacji z serwerami uwierzytelnienia i autoryzacji za pośrednictwem protokołów RADIUS, SecurID i LDAP w celu uwierzytelnienia i autoryzacji dostępu administracyjnego.
   xi) Musi pozwalać na obsłużenie minimum 8.000.000 jednoczesnych sesji/połączeń z prędkością zestawiania100.000 połączeń na sekundę.

b) **Wsparcie dla IPv6:**
   i) Rozwiązanie musi pozwalać na obsługę IPv6 przez moduł Firewall, Kontroli Aplikacji, Anty-malware, Filtrowania URL.
   ii) System musi być zgodny z poniższymi RFC dotyczącymi IPv6:
      (1) RFC 1981 Path Maximum Transmission Unit Discovery for IPv6
      (2) RFC 2460 IPv6 Basic specification
      (3) RFC 2464 Transmission of IPv6 Packets over Ethernet
      (4) RFC 4007 IPv6 Scoped Address Architecture
      (5) RFC 4193 Unique Local IPv6 Unicast Addresses
      (6) RFC 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers – wsparcie dla tuneli 6w4
      (7) RFC 4443 ICMPv6
      (8) RFC 4862 IPv6 Stateless Address Autoconfiguration

c) **Intrusion Prevention System (IPS) musi:**
   i) Posiadać możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system).
   ii) Posiadać możliwość pracy zarówno w trybie pasywnym (IDS) jak i aktywnym (IPS - z możliwością blokowania ruchu).
   iii) Posiadać możliwość wykrywania i uniemożliwiania szerokiej gamie zagrożeń (np.: złośliwe oprogramowanie, skanowanie sieci, ataki na usługi VoIP, próby przepełnienia bufora, ataki na aplikacje P2P, itp.).
   iv) Zapewniać co najmniej poniższe sposoby wykrywania zagrożeń:
      (1) Sygnatury ataków opartych na exploit'ach,
      (2) Reguły oparte na zagrożeniach,
      (3) Mechanizm wykrywania anomalii w protokołach.

v) Mieć możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakres protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzania zawartości pakietu
vi) Posiadać wiele możliwości reakcji na zdarzenia takie jak: tylko monitorowanie, blokowanie ruchu zawierającego zagrożenia, blokowanie adresów IP powiązanych z atakiem na określony czas;
vii) Posiadać możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji
viii) Zapewniać możliwość obrony przed atakami skonstruowanym tak, by uniknąć wykrycia przez IPS.
ix) Zapewniać mechanizm bezpiecznej aktualizacji sygnatur IPS, sygnatur AV oraz sygnatur do rozpoznawania aplikacji. Zestawy sygnatur/reguł muszą byś pobierane z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne
x) Zapewniać możliwość definiowania wyjątków dla sygnatur, a także zapewniać możliwość wyłączenia systemu przy określeniu adresów IP źródła lub przeznaczenia
xi) Urządzenie musi posiadać wbudowane narzędzie do tworzenia własnych sygnatur IPS.
xii) Musi mieć możliwość wykrywania anomalii w sieci. W tym celu musi mieć możliwość budowania profili normalnego stanu i zachowania sieci oraz identyfikowane odchylenia (m.in. nagłe odchylenia ilości zapytań i przekroczenie wartości progowych).
xiii) Musi pozwalać na pracę z przepustowością min. 3.6 Gbps mierzoną w warunkach typu Enterprise (Zamawiający nie dopuszcza urządzeń, gdzie wartość ta jest zdefiniowana jako „lab" „ideal" itp. zbliżone w nazwie definiujące warunki idealne lub laboratoryjne) przy uruchomionych co najmniej modułach Stateful Firewall, kontrola aplikacji, IPS, anty-wirus, anty-bot, filtrowanie URL
xiv) Musi posiadać dostępną publicznie informację o przepustowości urządzenia nie mniejszej niż 10 Gb/s mierzoną w warunkach typu Enterprise (Zamawiający nie dopuszcza urządzeń, gdzie w/w wartość jest zdefiniowana jako „lab" lub „ideal" itp. definiujące warunki idealne lub laboratoryjne) przy uruchomionych co najmniej modułach Stateful Firewall, kontrola aplikacji, IPS
xv) Pozwalać na ochronę protokołów VOIP

d) W zakresie **identyfikacji użytkownika (User Identity)** – urządzenie musi:
i) W oparciu o zdarzenia być zdolne do identyfikacji użytkownika poprzez zadanie zapytań do Microsoft Active Directory,
ii) Pozwalać na identyfikację i uwierzytelnianie użytkownika dla zasobów nie związanych z domeną,
iii) Integrować się z usługami katalogowymi RADIUS,
iv) Powodować minimalny wpływ na kontrolery domeny,

e) **System automatycznego wykrywania i klasyfikacji aplikacji wraz z filtrowaniem URL**:
i) Baza znanych aplikacji musi zawierać nie mniej niż 1800 pozycji. Urządzenie musi posiadać wbudowane narzędzie do tworzenia własnych sygnatur aplikacyjnych bez wsparcia producenta
ii) Urządzenie musi pozwalać na kategoryzację adresów URL w liczbie co najmniej 10.000.000.
iii) Rozwiązanie musi posiadać mechanizm ograniczenia użycia pasma per wszystkie polityki, jedną politykę lub adres IP
iv) Strona informująca o zablokowanym zasobie powinna być możliwa do zdefiniowania, dodatkowo powinna umożliwiać na przekierowanie użytkownika na inna stronę zewnętrzną.
v) Urządzenie musi wspierać mechanizmy białych i czarnych list.

f) **Wykrywanie malware oraz komunikacji z serwerami C&C:**
i) Moduł wykrywający malware i botnety powinien być zintegrowaną z platformą aplikacją.
ii) System Anti-Bot powinien umożliwiać wykrycie oraz blokadę podejrzanego zachowania w chronionych segmentach sieci.
iii) Wykrycie zdarzenia powinno opierać na wielowarstwowej analizie
iv) Musi istnieć możliwość stworzenia reguł dostępu bazujących na geolokalizacji adresu IP
v) System musi mieć wbudowaną funkcjonalność pozwalającą na odciążenie urządzenia, która sprawia że strony oraz serwery o wysokiej reputacji nie będą skanowane, a dostęp do serwerów lub stron o reputacji krytycznej będzie blokowany bez sprawdzania zawartości
vi) Urządzenie musi umożliwiać wykrycie malware poprzez statyczną i dynamiczną analizę próbki.
vii) Urządzenie musi mieć możliwość wysłania nieznanej mu próbki na dedykowany serwer sandbox (np. w chmurze) który na bazie zachowania próbki emulowanej w wielu środowiskach pozwoli na określenie jej stopnia zagrożenia
viii) Funkcjonalność powinna być zarządzana z centralnej konsoli.
ix) Funkcjonalność powinna posiadać możliwość inspekcji plików skompresowanych,

g) Inspekcja SSL/TLS (ruch przychodzący / wychodzący):
i) Wszystkie wymagane funkcje urządzenia odnośnie analizy ruchu na poziomie zawartości pakietów (payload) muszą być realizowane zarówno dla ruchu niezaszyfrowanego jak i zaszyfrowanego, przy użyciu protokołów: SSL 3,TLS 1.1, TLS 1.2 oraz TLS 1.3,

ii) Deszyfracja musi działać dla dowolnego połączenia zabezpieczonego SSL bądź TLS włączając w to połączenia HTTPS, IMAP4S, POP3S, SMTPS oraz SMTP ze STARTTLS.
iii) Inspekcja ruchu zaszyfrowanego, musi być możliwa do wyłączenia dla wybranych adresów.
iv) Funkcjonalność powinna pozwalać na wykorzystanie przez administratora filtrowania URL.

h) **Wykrywanie wiadomości SPAM:**
i) Mechanizmy wykrywania wiadomości SPAM powinny wykorzystywać dane o reputacji adresu IP nadawcy w celu uniknięcia fałszywej klasyfikacji.

i) **Brama IPSec VPN**:
i) Urządzenie powinno wspierać CA wewnętrzne oraz zewnętrzne.
ii) Wsparcie dla 3DES, AES, SHA2dla fazy IKE I i II oraz IKEv2 oraz 3DES, AES-GCM dla fazy II
iii) Wymagane jest także wsparcie protokołów ESP oraz AH
iv) Rozwiązanie musi obsługiwać wysokie grupy Diffie-Hellman, co najmniej 14, 15, 19 oraz 20
v) Rozwiązanie musi wspierać site-to-site VPN w następujących topologiach:
(1) gwiazda,
(2) punkt-punkt (point-to-point),
(3) połączenie poprzez huby.
vi) Urządzenie musi pozwalać na pracę z przepustowością 4.8Gbps dla VPN AES-128 mierzoną w warunkach laboratoryjnych.

j) **Ochrona przed wyciekiem informacji (Data Loss Prevention):**
i) Urządzenie musi umożliwiać zrealizowanie funkcjonalności pozwalającej na wykrywanie wycieków informacji (Data Loss Prevention).

3. Zarządzanie i monitorowanie

a) Definicje
i) Poprzez **zarządzanie** należy rozumieć konfigurację polityki bezpieczeństwa (polityka firewall, VPN, polityka ochrony antywirusowej, , ochrony przed atakami sieciowymi, atakami typu botnet, kontrola aplikacji), zarządzanie kontami administratorów i użytkowników, obsługę zdarzeń generowanych przez moduły zapór sieciowych.
ii) Poprzez **monitorowanie** należy rozumieć odczyt informacji dotyczących obsługiwanego ruchu sieciowego, min. natężenie ruchu, aktywne połączenia, zidentyfikowane, bieżące zagrożenia, statystyki ruchu i zagrożeń.

b) Wymagania:
i) Interfejsy zarządzania i monitorowania mogą być dostępne w jednym punkcie (GUI) bądź być rozdzielone.
ii) Zarządzanie oboma urządzeniami wykonywane jest wspólnie dla nich obu, tj. każda ww. zmiana wprowadzana jest jednokrotnie (np. na jednym z urządzeń) a odnosi skutek na obu urządzeniach.
iii) Dopuszczalne jest, jeśli w celu monitorowania należy się połączyć się z jednym z urządzeń, które jest w danej chwili aktywne (funkcja „active" w klastrze), pod warunkiem, że ta informacja jest dostępna w interfejsie zarządzania.
iv) Zarządzanie i monitorowanie są realizowane za pomocą co najwyżej 2-ch graficznych konsoli administratora (GUI) dostępnych pod systemem operacyjnym Windows. Konsola zarządzania posiada możliwości automatycznej weryfikacji spójności i niesprzeczności wprowadzonej polityki bezpieczeństwa.
v) Komunikacja pomiędzy GUI zarządzania i monitorowana a urządzeniami jest szyfrowana protokołem SSL/TLS
vi) Uwierzytelnianie administratorów do GUI zarządzania i monitorowania odbywa się za pomocą haseł statycznych lub haseł dynamicznych lub certyfikatów cyfrowych. Istnieje możliwość definiowania szczegółowych uprawnień administratorów , co najmniej pełne uprawnienia i uprawnienia tylko do odczytu.
vii) Interfejs monitorowania jest w stanie wyświetlić w GUI listę aktywnych połączeń obsługiwanych przez moduły zapór sieciowych. Informacja o połączeniu powinna zawierać minimum adres źródła, adres przeznaczenia, port źródła, port przeznaczenia oraz identyfikator usługi sieciowej.
viii) Interfejs monitorowania umożliwia wyszukiwanie i filtrację zdarzeń wygenerowanych przez moduły zabezpieczeń. Administrator jest w stanie zdefiniować własne szablony wyszukiwania i wyświetlania zdarzeń.
ix) Interfejs monitorowania umożliwia monitorowanie i prezentowanie za pomocą graficznej konsoli takich parametrów sprzętowych zarządzanych zapór sieciowych jak: średnie obciążenie procesora, wersję oprogramowania zapory sieciowej, nazwę i wersję zainstalowanej polityki bezpieczeństwa.
x) Interfejs monitorowania umożliwia graficzne wyświetlanie statystyk ruchu sieciowego, przetwarzanego przez zapory sieciowe, takich jak: najczęściej wykorzystywane usługi sieciowe, najczęstsze źródła transmisji, najczęstsze adresy docelowe, aktywne i zerwane tunele VPN.

xi) Interfejs zarządzania musi posiadać funkcjonalność składowania poprzednich wersji konfiguracji, by w łatwy sposób można je było przywrócić na urządzenie

4. Licencje

a) Wymagania dotyczące licencji
   i) Jeśli do realizacji wymaganych funkcji klastra firewalli potrzebne są licencje bądź subskrypcje, to należy je dostarczyć wraz z klastrem. Licencje /subskrypcje muszą posiadać ważność 60 miesięcy.
   ii) Firewalle wchodzące w skład klastra muszą być objęte serwisem producenta na okres 60 miesięcy. W ramach serwisu muszą być dostępne następujące usługi: dostęp do aktualizacji oprogramowania systemowego, dostęp do wsparcia technicznego realizowanego w języku polskim oraz wymiana urządzeń w przypadku awarii.

5. Dojrzałośc produktu:

a) Zaoferowany system UTM musi być produktem obecnym na rynku IT od co najmniej 3 lat oraz stanowić kompletne rozwiązanie sprzętowo-programowe, w szczególności:
   i) Producent systemu UTM musi być odnotowywany w zestawieniach i raportach uznanych organizacji działających w sektorze usług i systemów IT, w tym minimum: w raportach firmy Gartner za lata 2018, 2019 i 2020; dla roku 2020 należy odnosić się do raportu „Gartner Magic Quadrant for Network Firewalls" (adres dostępowy do dokumentu – data pobrania 2020.12.20: https://www.gartner.com/en/documents/3961528);
   ii) Uwaga! Wymóg ten dotyczy oprogramowania systemu UTM; dopuszczalne jest zaoferowanie systemu UTM w oparciu o nowe modele serwerów niespełniające wymogu dostępności od 3 lat na rynku, jednakże zgodne z oprogramowaniem systemu UTM, tj. znajdujące się na liście kompatybilności tego oprogramowania;

4.b. Sieć SAN

Sieć SAN obejmuje sieć komunikacyjną o niskiej przepustowości zbudowaną w oparciu o przełączniki SAN/FC, dedykowaną dla połączenia serwerów systemu wysokiej dostępności oraz systemu baz danych NoSQL z elementami macierzy centralnej (dyskowej) realizującymi usługi przechowywania blokowego; połączenia te zapewnią wydajna komunikację pomiędzy serwerami a urządzeniami dyskowymi, z możliwością wykorzystania wielu ścieżek fizycznych oraz realizacji mechanizmów wysokiej niezawodności połączeń i dostępu do danych.

Elementy sieci SAN muszą spełniać co najmniej poniższe wymagania dotyczące cech i funkcjonalności przełączników sieciowych, topologii sieci – przy czym wszystkie wymagania muszą być traktowane jako minimalne, chyba że treść wymogu stanowi inaczej.

4.b.1 Przełączniki sieci SAN

Należy dostarczyć minimum 2 przełączniki w technologii Fibre Channel o przepustowości portów min.16Gbit/s.

1. Wymagania ogólne

a) dostarczyć nie mniej niż: 2 przełączniki sieci SAN wykonane w technologii Fibre Channel o przepustowości 16Gbit/s lub szybszej;
b) Wymagana jest dostawa takiej liczby przełączników sieci SAN, która umożliwia realizację wymaganej topologii połączeń w sieci SAN oraz przepustowości połączeń miedzy serwerami a macierzą centralną;
c) Przełączniki sieci SAN muszą być konfigurowane i dostarczane parami, tzn. należy dostarczyć liczbę przełączników, która jest wielokrotnością liczby 2, dla zachowania pełnej niezależności redundantnych ścieżek komunikacyjnych pomiędzy serwerami a macierzą centralną oraz statystycznej symetryczności obciążenia przełączników redundantnymi ścieżkami komunikacyjnymi łączącymi serwery z macierzą;

2. Topologia sieci:

c) Topologia wymaganych połączeń w sieci SAN:
   i) Przełączniki sieci SAN muszą zapewniać niezawodne i redundantne połączenia serwerów systemu wysokiej dostępności oraz serwerów systemu baz danych noSQL z elementami macierzy centralnej (dyskowej) realizującymi usługi przechowywania blokowego;
   ii) Topologia połączeń musi umożliwiać wielościeżkowego dostępu z serwera fizycznego i/lub wirtualnego do wolumenów blokowych na macierzy dyskowej (centralnej) – tzw. *multipathing*;
   iii) Zastosowane przełączniki (liczba, typ, przepustowość, liczba portów) oraz topologia połączeń muszą umożliwiać pracę portów serwerów z pełną przepustowością umożliwiającą strumieniową transmisję przez te porty danych pomiędzy dowolnym serwerem systemu wysokiej dostępności lub serwerem systemu baz danych NoSQL a macierzą dyskową (centralną) z wydajnością minimum 1,5GB/s (Gigabajta) na sekundę per serwer (w jednym kierunku);

iv) Po wykonaniu wymaganych połączeń w każdym przełączniku SAN musi pozostać **rezerwa minimum 25% portów** do podłączania serwerów i urządzeń do macierzy; porty te muszą być obsadzone wkładkami (identycznymi jak porty wykorzystane do połączeń) oraz aktywowane;

3. Wymagania dla przełączników sieci SAN:

b) **Wymagania dla przełączników sieci SAN** (16Gbit/s lub 32Gbit/s):

i) porty do podłączania serwerów – wymagania minimalne:
(1) liczba portów do podłączania serwerów: **48**
(2) przepustowość każdego z portów do podłączania serwerów 16Gbit/s lub wyższa (np. 32Gbit/s)

ii) Funkcjonalność przełączników:
(1) Przełącznik FC musi być wykonany w technologii FC 16 Gbit/s lub szybszej
(2) Przełącznik musi mieć możliwość pracy portów FC z przepustowością z niższymi od 16Gbit/s prędkościami (16, 8, 4, 2 Gbit/s) oraz wspierać funkcję autonegocjacji;
(3) Przełącznik musi być kompatybilny z dostarczonymi serwerami systemu wysokiej dostępności i systemu baz danych a także z dostarczoną macierzą dyskową (centralną);
(4) Wsparcie dla polityka monitorowania i alarmowania (MAPS)
(5) Wsparcie dla Dynamic Fabric Provisioning (DFP) oraz Dynamicznego wyboru ścieżki (DPS)
(6) Wsparcie dla przekierowania ramek
(7) Wsparcie dla agregacja w oparciu o ramki FSPF
(8) Wsparcie dla blokowania portów
(9) Rejestracja informacji o zmianie stanu (RSCN)
(10) Wsparcie dla funkcjonalności serwera prostych nazw (SNS)
(11) Zarządzanie przez SSH; wsparcie dla zarządzania i monitorowania przełącznika out-of-band za pomocą dedykowanych interfejsów/portów podłączonych do sieci LAN do zarządzania;
(12) wsparcie dla OpenFlow1.3 lub innych technologii SDN (ang. Software Defined Network)

iii) Architektura logiczna / wydajność:
(1) Przepustowość przełącznika SAN musi wynosić minimum 640 Gbit/s end-to-end full duplex
(2) Musi być możliwe łączenie przełączników FC w tzw. fabric (poprzez porty typu E)

iv) Wszystkie wolne porty przełączników SAN muszą być aktywowane (mieć dostarczoną licencję) oraz być wyposażone w odpowiednie wkładki optyczne oraz posiadać licencje pozwalające na realizację zdefiniowanej powyższymi wymaganiami funkcjonalności przełącznika;

4.c. Sieć LAN dla pracowni i czytelni

Sieć LAN dla pracowni digitalizacyjnych i czytelni Biblioteki Śląskiej obejmuje przełączniki LAN w technologii Ethernet o przepustowości 10/40 (25/100) Gbit/s umożliwiające podłączenie stacji roboczych zlokalizowanych w pomieszczeniach pracowni do sieci LAN dla infrastruktury serwerowej, zapewniając odpowiednią wydajność dostępu do usług infrastruktury serwerowej z poziomu pracowni Biblioteki Śląskiej.

Elementy sieci LAN dla pracowni digitalizacyjnych oraz czytelni muszą spełniać co najmniej poniższe wymagania dotyczące cech i funkcjonalności przełączników sieciowych oraz topologii sieci – przy czym wszystkie wymagania muszą być traktowane jako minimalne, chyba że treść wymogu stanowi inaczej.

1. Wymagania ogólne dla sieci LAN dla pracowni:

b) Wymagana jest dostawa takiej liczby przełączników sieci LAN, która umożliwia realizację wymaganej topologii połączeń w sieci LAN dla pracowni i czytelni, umożliwiającej podłączenie stacji roboczych zlokalizowanych w pomieszczeniach pracowni i czytelni Biblioteki Śląskiej do sieci LAN dla infrastruktury serwerowej, przy czym należy dostarczyć nie mniej niż:

i) **3** przełączniki **40-portowe** sieci LAN dla pracowni 10/40 (25/100) Gigabit Ethernet – po jednym dla pracowni digitalizacyjnych oraz dwóch czytelni cyfrowych;

ii) do przełączników tych będą podłączane stacje robocze zlokalizowane w pracowniach i czytelniach:
(1) Szafa LPD01 – Pracowania Digitarium: 38 stacji roboczych
(2) Szafa LPD 02 – Czytelnia Główna: 30 stacji roboczych
(3) Szafa LPD 03 – Czytelnia Czasopism: 20 stacji roboczych

2. Topologia sieci LAN dla pracowni:

d) Przełączniki sieci LAN dla pracowni muszą zapewniać połączenia stacji roboczych zlokalizowanych w pomieszczeniach pracowni Biblioteki Śląskiej z siecią LAN dla infrastruktury serwerowej;

e) Zastosowane przełączniki (liczba, typ, przepustowość, liczba portów) oraz topologia połączeń muszą umożliwiać równoczesną pracę **przynajmniej 4 stacji roboczych równocześnie** per każdy przełącznik LAN dla pracowni z pełną przepustowością portów tych stacji roboczych, umożliwiającą strumieniową

transmisję przez te porty danych pomiędzy stacjami roboczymi a serwerami systemu wysokiej dostępności i/lub systemu baz danych NoSQL **z wydajnością minimum 0,8GB/s** (Gigabajta na sekundę) per stacja robocza (w jednym kierunku);

f) Po wykonaniu wymaganych połączeń w każdym przełączniku LAN dla pracowni musi pozostać **rezerwa minimum 8 portów** wolnych (od strony stacji roboczych, nie dotyczy tzw. uplinków); porty te muszą być obsadzone wkładkami (identycznymi jak porty do stacji) oraz aktywowane;

3. Wymagania dla przełączników sieci LAN dla pracowni:

a) **Wymagania dla każdego z przełączników sieci LAN dla pracowni** (10/25/40/100Gbit) – p*rzełączniki sieci LAN da pracowni muszą spełniać wymagania zdefiniowane dla przełączników sieci LAN produkcyjnej zdefiniowane w punkcie 4.a.1.3.a) z wyłączeniem następujących punktów:*

i) porty do podłączania stacji roboczych – wymagania minimalne:
   (1) liczba portów do podłączania stacji roboczych: **48**
   (2) przepustowość każdego z portów do podłączania stacji roboczych **10Gbit;**

ii) porty uplink – do przełączników sieci LAN dla infrastruktury serwerowej – wymagania minimalne:
   (1) liczba uplinków przypadających na każde 48 portów do stacji roboczych: **4**
   (2) przepustowość każdego z portów uplink min. **10Gbit/**s lub wyższa (np. 25 lub 40 Gbit/s)

iii) połączenia / instalacja:
   (1) porty uplink przełączników sieci LAN dla pracowni będą połączone z portami „serwerowymi" przełączników sieci LAN dla infrastruktury serwerowej poprzez posiadane przez Zamawiającego przełącznice optyczne typu: R&M Unirack 1U 24/12xLC Duplex OM4 (https://www.rdm.com/R-M-Products/Fiber-Optics/19-patch-panels/19-UniRack/19-1U-UniRack-12xLC-Duplex/19-1U-UniRack-12xLC-Duplex-OM4-PC-ceramic-Bm-3), połączone kablami typu R&M R852313 (https://www.rdm.com/R-M-Products/Fiber-Optics/Installation-Cables/CLT-Standard-Duct-Cable-up-to-12-fibers-universal-use-Dca-grading/Central-loose-tube-cable-universal-use-no-armour-FRLSZH-sheath-green-Dca-01x12-fibers-OM4)
   (2) przełączniki *sieci LAN da pracowni i czytelni* umieszczone będą, wraz z przełącznicami optycznymi w Lokalnych Punktach Dystrybucyjnych, zorganizowanych w posiadanych przez Zamawiającego szafach (szer. x głęb. x wys.: 60cm x 60cm x 12U) podwieszonych w pomieszczeniach pracowni i czytelni (link do specyfikacji szaf: http://szafy-serwerowe.com.pl/wp-content/uploads/2017/07/seria_wd-1.pdf);
   ***Uwaga**! Zamawiający posiada w pomieszczeniach pracowni i czytelni szafy o głębokości zewnętrznej **60**cm. Zaoferowane przełączniki muszą być zainstalowane w tych szafach wraz z okablowaniem zasilającym i sieciowym, ułożonym zgodnie z dobrymi praktykami, w tym m.in. z zachowaniem minimalnych promieni gięcia dla okablowania światłowodowego*

5. SYSTEM DO WYKONYWANIA KOPII ZAPASOWYCH

Dane systemu wysokiej dostępności dostarczanego w ramach niniejszego zamówienia, muszą być zabezpieczane poprzez wykonywanie kopii zapasowych z replikacją do Centrum Zapasowego Biblioteki Śląskiej. Ponadto, w przypadku zaoferowania platformy wirtualizacyjnej dla systemu baz danych NoSQL, platforma ta i maszyny wirtualne w niej skonfigurowane muszą także być objęte analogicznym zabezpieczeniem.

Poniżej opisane są wymagania minimalne dla systemu wykonywania kopii zapasowych

1. Architektura systemu do wykonywania kopii zapasowych:

1) Oprogramowanie do wykonywania kopii zapasowych musi mieć elastyczną architekturę umożliwiającą:
   a. zabezpieczanie maszyn wirtualnych działających na systemie wysokiej dostępności oraz zabezpieczanie danych platformy wirtualizacyjnej systemu wysokiej dostępności (konfiguracja, stany) poprzez wykonywanie zreplikowanych geograficznie kopii zapasowych dla danych przechowywanych w systemie wysokiej dostępności oraz w centralnej macierzy dyskowej;
   b. jeśli w ramach rozwiązania dostarczane jest rozwiązanie do wirtualizacji serwerów systemu baz danych NoSQL to system do wykonywania kopii zapasowych musi umożliwiać zabezpieczanie danych tego środowiska w sposób analogiczny do zabezpieczenia danych systemu wysokiej dostępności;
   c. wykorzystanie jako opcjonalnego elementu systemu wykonywania kopii zapasowych deduplikatorów sprzętowych;
   d. wykonywanie kopii zapasowych dla wymaganego wolumenu danych zgodnie ze zdefiniowanym schematem i harmonogramem backupów oraz wymaganym oknem retencji, wraz z replikacją danych, a także odtwarzanie danych kopii zapasowej w założonym oknie czasowym; należy zapewnić, że wymóg ten będzie spełniony w środowisku dwóch centrów danych Biblioteki Śląskiej tj. Centrum Podstawowego i Centrum Zapasowego, pomiędzy którym replikowane są dane kopii zapasowych;
2) Architektura i funkcjonalność rozwiązania musi umożliwiać bezpieczne *składowanie zawartości kopii zapasowych danych* maszyn wirtualnych i platformy wirtualizacyjnej systemu wysokiej dostępności (oraz opcjonalnie systemu baz danych NoSQL), tzn. składowanie ich w sposób zapewniający odporność tych kopii na awarie systemu wysokiej dostępności, podsystemu dyskowego serwerów systemu wysokiej dostępności oraz centralnej macierzy dyskowej, poprzez replikowanie danych kopii zapasowej pozyskanych w Centrum Podstawowym Biblioteki Śląskiej do Centrum Zapasowego, w ramach procesu wykonywania kopii zapasowej lub asynchronicznie, natychmiast po zakończeniu wykonywania kopii zapasowej.
3) Architektura rozwiązania musi umożliwiać efektywne odtwarzanie danych, zapewniające odtworzenie pełnego środowiska produkcyjnego lub poszczególnych maszyn wirtualnych w systemie wysokiej dostępności (oraz w systemie baz danych NoSQL jeśli dla serwerów tego systemu zaoferowano platformę wirtualizacyjną) a także na macierzy dyskowej (centralnej) we wskazanym poniżej czasie.

2. Funkcjonalność systemu do wykonywania kopii zapasowych:

1) System musi obsługiwać tj. wykonywać i przechowywać kopie zapasowe oraz umożliwiać odtwarzanie maksymalnie **250TiB** danych przechowywanych w systemie wysokiej dostępności (oraz w systemie baz danych NoSQL jeśli dla serwerów tego systemu zaoferowano platformę wirtualizacyjną) a także macierzy dyskowej (centralnej) – dla założonego harmonogramu kopii i okna retencji.
2) Jeśli Wykonawca zaoferował rozszerzenie pojemności pamięci dyskowych (magnetycznych, HDD) w macierzy dyskowej (centralnej), to system wykonywania kopii zapasowych musi obsługiwać tj. wykonywać i przechowywać kopie zapasowe oraz umożliwiać odtwarzanie wolumenu danych o wielkości właściwej dla zaoferowanej pojemności całkowitej (tj. sumy przestrzeni pamięci flash oraz pamięci magnetycznych HDD) macierzy dyskowej (centralnej) – maksymalnie 450TiB danych – dla założonego harmonogramu kopii oraz okna retencji;
3) Należy zapewnić odpowiednie licencje, przestrzeń fizyczną, architekturę i funkcjonalność systemu do wykonywania kopii zapasowych umożliwiające spełnienie wymagań zdefiniowanych w ppkt. 1) i 2).
4) Wymagane jest wykonywanie kopii zapasowych dla danych maszyn wirtualnych działających w systemie wysokiej dostępności (oraz w systemie baz danych NoSQL, jeśli dla serwerów tego systemu zaoferowano platformę wirtualizacyjną) a także danych bieżących (np. stan, konfiguracja) platformy wirtualizacyjnej.
5) Harmonogram wykonywania kopii zapasowych obejmuje:
   a. wykonywanie codziennej kopii przyrostowej (w nocy, w dni robocze);
   b. wykonywanie tygodniowej pełnej kopii danych (dla każdego zbioru danych rotacyjnie, co najmniej 1 raz w miesiącu w ciągu weekendu, poza godzinami typowej aktywności użytkowników systemu);

6) Okno backupowe:
   a. wykonanie codziennej kopii zapasowej danych musi mieścić się w oknie backupowym o długości maksimum **8** godzin (zakłada się dobową zmienność danych na poziomie maksimum **1%**),
   b. wykonanie pełnej kopii zapasowej dla zbioru danych dla którego na dany weekend przypada wykonanie pełnej kopii musi się mieścić w oknie backupowym o długości **12** godzin.
7) Okres retencji dla danych kopii zapasowych wynosi **21 dni.**
8) Czasy odtwarzania:
   a. Całkowite odtworzenie środowiska (konieczne np. w przypadku wystąpienia awarii sprzętowej lub logicznej systemu wysokiej dostępności i/lub jego podsystemu dyskowego, systemu baz danych NoSQL – jeśli dla serwerów tego systemu zaoferowano platformę wirtualizacyjną i/lub macierzy dyskowej/centralnej), w tym maszyn wirtualnych i aplikacji systemu wysokiej dostępności (oraz systemu baz danych NoSQL jeśli dla serwerów tego systemu zaoferowano platformę wirtualizacyjną) musi być możliwe w czasie nie dłuższym niż **48** godzin;
   b. Odtworzenie pojedynczej maszyny wirtualnej musi być możliwe w czasie nie dłuższym niż **4** godziny – *zakładając,* że wolumen danych pojedynczej maszyny to maksymalnie **2TB**.
9) Wykorzystanie łącza sieciowego:
   a. Przepustowość połączenia sieciowego pomiędzy Centrum Podstawowym oraz Centrum Zapasowym Biblioteki Śląskiej to **10GBit/s**.
   b. Podczas normalnego użytkowania, na potrzeby wykonywania przyrostowych kopii zapasowych danych oraz odtwarzania mniejszych awarii (maszyna wirtualna, pojedyncze pliki/katalogi) łącze może zostać wykorzystane do 70% przepustowości standardowej tego łącza, w godzinach nocnych;
   c. Do odtwarzania danych, w przypadku rozległej awarii łącze może zostać wykorzystane do 90% przepustowości tego łącza, niezależnie od pory dnia – zarówno w dzień jak i w nocy;
   d. *Ograniczanie wykorzystywanego pasma musi być możliwe z poziomu systemu backupowego*.
10) Funkcjonalności systemu do wykonywana kopii zapasowych – system musi umożliwiać:
   a. automatyczne wykonywanie kopii zapasowych wg harmonogramu opartego na kalendarzu;
   b. wykonywania kopii typu: pełna, przyrostowa, różnicowa;
   c. definiowanie harmonogramów wykonywania kopii zapasowych umożliwiających rotacyjne wykonywanie kopii pełnych danych w różnych tygodniach dla różnych zbiorów danych;
   d. wykonywanie kopii zapasowych otwartych plików (dotyczy systemów operacyjnych Windows);
   e. wykonywanie kopii zapasowych systemu Active Directory oraz Microsoft Sharepoint;
   f. wykonywanie kopii zapasowych maszyn wirtualnych z wykorzystaniem mechanizmów optymalizujących ilość danych pobieranych z wolumenów maszyn wirtualnych i przesyłanych do systemu kopii zapasowych – tzw. ang. CBT (*Change Block Tracking*) lub innego, równoważnego mechanizmu zapewniającego, że w ramach tworzenia kopii przyrostowej danych pobierane z wolumenów maszyn wirtualnych oraz przesyłane do systemu kopii zapasowych będą tylko bloki zmienione od ostatniego backupu (całościowego lub przyrostowego);
   g. wykonywanie kopii zapasowych całych maszyn wirtualnych (obrazów wolumenów) oraz możliwość granularnego odtwarzania danych z backupu, włączając możliwość odtworzenia pojedynczej maszyny wirtualnej oraz możliwość odtworzenia pojedynczych plików lub wskazanych katalogów;
   h. deduplikację danych na poziomie blokowym – wykonywaną *online*, tj. podczas tworzenia kopii zapasowej danych – mechanizm musi być integralną częścią systemu do wykonywania kopii zapasowych z punktu widzenia jego architektury i technologii – może być jednak opcją z punktu widzenia handlowego; jeśli dla mechanizmu deduplikacji wymagana jest licencja, musi być ona dostarczona w typie i ilości odpowiadającej potrzebom tworzenia kopii zapasowych danych serwera produkcyjnego, *przy czym to na Wykonawcy spoczywa obowiązek udowodnienia, że zaoferowana pojemność systemu wykonywania kopii zapasowych po deduplikacji odpowiada tym potrzebom, tj. umożliwia składowanie kopii zapasowych dla wszystkich zabezpieczanych danych serwera produkcyjnego oraz ich wersji przy założonym okresie retencji danych (wymagane jest załączenie do oferty wydruku wyliczeń/analizy z konfiguratora rozwiązania do backupu/deduplikacji lub wyliczeń pojemności potwierdzonych przez producenta tych rozwiązań);*
   i. uruchamianie skryptów przed i po wykonywaniu kopii zapasowych – przy czym uruchamianie skryptów musi być automatyczne, koordynowane z procesem wykonywania kopii zapasowej;
11) Kompatybilność z systemami operacyjnymi i środowiskami do wirtualizacji:
   a. rozwiązanie do wykonywania kopii zapasowych danych musi znajdować się na liście wsparcia wymienionych systemów lub posiadać udokumentowane na stronach producenta wsparcie co najmniej dla wymienionych systemów: systemy operacyjne Windows Server 2016 i nowsze, Redhat Enterprise Linux wersja 8 i nowsze lub Suse Linux Enterprise Server 15 i nowsze; środowiska wirtualizacyjne: VMware vSphere 7.0 i nowsze lub RedHat Virtualization 4.0 i nowsze, Hyper-V dla Windows Server 2016 i nowsze;

b. wspierane w zaoferowanym rozwiązaniu do wykonywania kopii zapasowych systemy operacyjne i środowiska do wirtualizacji muszą być kompatybilne z zaoferowanymi dla serwera systemu wysokiej dostępności systemami operacyjnymi i środowiskiem wirtualizacji (oraz z zaoferowanymi dla serwerów systemu baz danych NoSQL systemami operacyjnymi i środowiskiem wirtualizacji – jeśli zaoferowano platformę wirtualizacyjną dla serwerów systemu baz danych NoSQL);
c. Oprogramowanie musi integrować się bezpośrednio z zaoferowaną w ramach rozwiązania macierzą dyskową (centralną) zapewniając możliwość tworzenia kopii zapasowych z bezpośrednim wykorzystaniem migawek (tzw. ang. *snapshot*) na poziomie macierzy dyskowej (centralnej). Oprogramowanie musi umożliwiać odtwarzanie maszyn wirtualnych z kopii zapasowej z wykorzystaniem migawek, w sposób skoordynowany z zaoferowaną platformą wirtualizacyjną.

12) Zarządzanie:
a. System do wykonywania kopii zapasowych musi być wyposażony w interfejs graficzny (GUI) do zarządzania umożliwiający minimum konfigurowanie trybu i parametrów zabezpieczania kopią zapasową maszyn wirtualnych, definiowanie i przypisywanie schematów backupu do zabezpieczanych maszyn wirtualnych, zarządzanie politykami kopii zapasowych, zarządzanie pulami mediów oraz schematami kopiowania/replikacji i migracji danych między tymi pulami;
b. System musi posiadać funkcje bieżącego monitoringu, w tym wykrywać i alarmować operatora o błędach (np. niewykonanie kopii zapasowej) lub przekroczeniu wartości progowych parametrów;
c. System musi umożliwiać tworzenie raportów i podsumowań dla zadań backupu;
d. System musi umożliwiać podgląd stanu zadań backupowych (stan: np. aktywne/nieaktywne, status zakończenia) oraz zadań odtwarzania danych (stan, status zakończenia).

13) Zabezpieczenie danych systemu wykonywania kopii zapasowych:
a. System wykonywania kopii zapasowych musi mieć wbudowane mechanizmy zabezpieczania konfiguracji tego systemu i umożliwiać szybkie odtwarzanie stanu systemu wykonywania kopii zapasowych w przypadku jego awarii lub ponownej instalacji.
b. Mechanizm zabezpieczenie danych systemu wykonywania kopii zapasowych musi umożliwiać odtworzenie systemu kopii zapasowych oraz danych kopii zapasowych nawet w przypadku całkowitej, rozległej awarii w Centrum Podstawowym, na bazie informacji konfiguracyjnych oraz danych kopii zapasowej przechowywanych w Centrum Zapasowym.

14) Sieć i bezpieczeństwo komunikacji:
a. System musi posiadać wbudowaną możliwość szyfrowania danych przesyłanych przez sieć LAN/WAN, z wykorzystaniem protokołów SSL/TLS, minimum pomiędzy klientem kopii zapasowych a serwerem systemu wykonywania kopii zapasowych. Funkcjonalność ta musi być zintegrowana w systemie backupu. Rozwiązanie, w którym zabezpieczenie transmisji danych w ramach systemu kopii zapasowych wymaga użycia zewnętrznych mechanizmów (np. VPN, IPSec) nie jest akceptowane.

3. Komponenty sprzętowe systemu wykonywania kopii zapasowych

1) Architektura komponentów fizycznych:
a. Architektura komponentów fizycznych – węzły (serwery, appliance) i elementów sieci LAN/SAN (jeśli taka sieci jest wymagana i jest integralna częścią rozwiązania) systemu wykonywania kopii zapasowych – musi spełniać podstawowe wymagania związane z architekturą zdefiniowane dla komponentów serwerowych (systemu wysokiej dostępności, systemu baz danych) oraz sieciowych (sieci LAN/SAN), w szczególności, wszystkie elementy systemu wykonywania kopii zapasowych muszą być redundantne:
i. napędy dyskowe w węzłach (serwerach, appliance) systemu wykonywania kopii zapasowych – muszą być redundantne i zapewniać możliwość realizacji nadmiarowego przechowywania danych oraz przejmowania obsługi żądań I/O w przypadku awarii pojedynczych komponentów;
ii. Interfejsy i przełączniki sieci LAN/SAN (jeśli wymagane) – muszą zapewniać możliwość skonfigurowania redundantnych połączeń sieciowych w ramach systemu wykonywania kopii zapasowych oraz pomiędzy klientami systemu wykonywania kopii zapasowych a systemem wykonywania kopii zapasowych;
iii. Zasilacze i wentylatory węzłów i przełączników – muszą zapewniać zasilanie i chłodzenie komponentów fizycznych systemu backupowego pomimo awarii jednej z linii zasilania;
iv. kontrolery dyskowe w węzłach (serwerach, appliance) systemu wykonywania kopii zapasowych muszą zabezpieczać zawartość buforów do zapisu w przypadku nagłego zaniku zasilania;
v. węzły systemu wykonywania kopii zapasowych (serwery, appliance) – muszą wpierać automatyczne wyłączanie w odpowiedzi na zgłoszoną przez UPS awarię zasilania sieciowego;

2) Parametry minimalne komponentów sprzętowych systemu wykonywania kopii zapasowych:
a. Napędy dyskowe / dyski magnetyczne (HDD) dla danych kopii zapasowych:
i. Dopuszczalne technologie dysków magnetycznych (HDD): NL-SAS lub SATA;
ii. Możliwość wykorzystania dysków o pojemności 12TB, 14TB i 16TB.

iii. Dysk klasy enterprise: Minimalny MTBF [godzin]: 2 000 000

b. Napędu flash (SSD/NVMe) dla meta-danych systemu wykonywania kopii zapasowych:
   i. Dopuszczalne technologie pamięci flash (SSD/NVMe): SAS, PCIe, M.2, SATA
   ii. Dysk klasy enterprise: Minimalny MTBF [godzin]: 2 000 000
   iii. Minimalna odporność na ścieranie [DWPD (ang. *disk writes per day*)]: 3

c. Interfejsy sieciowe:
   i. system wykonywania kopii zapasowych musi wykorzystywać do komunikacji standardowe interfejsy sieciowe, w technologii Ethernet o przepustowości 10Gbit lub wyższej, umożliwiające wykorzystanie minimum następujących funkcjonalności: duże ramki (*Jumbo Frames*), agregacja linków (LACP), sieci wirtualne VLAN (802.1Q),
   ii. W przypadku, gdy dla uzyskania wymaganej wydajności w środowisku produkcyjnym (poza laboratorium), konieczne jest wykorzystanie wielu interfejsów sieciowych, węzły systemu wykonywania kopii zapasowych muszą być zaoferowane w konfiguracji zapewniającej agregację tych interfejsów, z uwzględnieniem cech i funkcji zaoferowanych przez Wykonawcę przełączników LAN sieci produkcyjnej dla infrastruktury serwerowej oraz zastosowanej w projekcie topologii tej sieci;

3) Aspekty fizyczne komponentów systemu wykonywania kopii zapasowych: obudowy, montaż, okablowanie:
   a. węzły (serwery, appliance) systemu wykonywania kopii zapasowych muszą być wyposażone w redundantne zasilacze i wentylatory. W każdym z węzłów redundantne zasilacze muszą mieć możliwość zasilania z różnych źródeł, bez potrzeby użycia zewnętrznych urządzeń.
   b. Elementy systemu wykonywania kopii zapasowych muszą być montowalne w zaoferowanych przez Wykonawcę szafach przemysłowych 19”. Architektura rozwiązania musi być tak dobrana, by system wykonywania kopii zapasowych w zaoferowanej pojemności mógł być zainstalowany wraz z pozostałymi elementami infrastruktury serwerowej w 3 szafach rack w Centrum Podstawowym oraz 1 szafie rack w Centrum Zapasowym.
   c. System wykonywania kopii zapasowych musi wykorzystywać dedykowane interfejsy sieciowe w serwerach systemu wysokiej dostępności oraz w serwerach systemu baz danych NoSQL (jeśli taki dla serwerów systemu baz danych NoSQL zaoferowano rozwiązanie do wirtualizacji) do obsługi ruchu związanego z wykonywaniem kopii zapasowych oraz odtwarzaniem danych z backupu – w celu zagwarantowania dedykowanej przepustowości ruchu backupowego i jego separacji od ruchu produkcyjnego do/z aplikacji, usług i narzędzi działających w systemie wysokiej dostępności i systemie baz danych NoSQL;
   d. Wraz z elementami sprzętowymi rozwiązania (węzły, elementy sieci) należy dostarczyć okablowanie zasilające i sieciowe, w tym dla sieci LAN i SAN (jeśli wymagane dla połączeń wewnętrznych); elementy sprzętowe systemu wykonywania kopii zapasowych muszą być wyposażone w uchwyty umożliwiające ułożenie okablowania zgodnie z dobrymi praktykami; w szczególności dla okablowania optycznego – prowadnice pozwalające na ułożenie okablowania optycznego z zachowaniem minimalnych promieni gięcia oraz eliminujące naprężenia okablowania podczas wykonywania czynności serwisowych takich jak wysuwanie serwerów lub appliance czy wymiana dysków;

4. Dojrzałość produktu:
   a. Zaoferowany system wykonywania kopii zapasowych musi być produktem obecnym na rynku IT **od co najmniej 3 lat** oraz stanowić kompletne rozwiązanie sprzętowo-programowe
   b. Producent systemu wykonywania kopii zapasowych musi być odnotowywany w zestawieniach i raportach uznanych organizacji działających w sektorze usług i systemów IT, w tym minimum: w raportach firmy Gartner za lata 2018, 2019 i 2020; dla roku 2020 należy odnosić się do raportu „Magic Quadrant for Data Center Backup and Recovery Solutions” (adres dostępowy do dokumentu: https://www.gartner.com/en/documents/3987618);
   c. Uwaga! Wymóg ten dotyczy oprogramowania systemu wykonywania kopii zapasowych; dopuszczalne jest zaoferowanie system wykonywania kopii zapasowych w oparciu o nowe modele węzłów (serwery, appliance), niespełniające wymogu dostępności od 3 lat na rynku, jednakże zgodne z oprogramowaniem do wykonywania kopii zapasowych, tj. znajdujące się na liście kompatybilności tego oprogramowania;
   d. Zaoferowany system wykonywania kopii zapasowych musi być produktem gotowym, posiadającym na moment składania oferty wszystkie wymagane przez Zamawiającego funkcjonalności, opisane w powszechnie dostępnej dokumentacji rozwiązania (specyfikacje, katalogi, dokumentacja techniczna, tzw. *white-paper*);

6. SYSTEM DO ZARZĄDZANIA KOMPUTERAMI

Wraz z infrastrukturą serwerową Wykonawca musi dostarczyć system do zarządzania komputerami, spełniające zdefiniowane poniżej minimalne wymagania dla tego oprogramowania.

6.a. Oprogramowanie do zarządzania komputerami

1. Wymagania ogólne:

a) Oprogramowanie musi posiadać budowę modułową, składającą się z serwera zarządzającego, zdalnych konsoli oraz agentów. Komunikacja pomiędzy serwerem a agentami i konsolami nawiązywana musi być przy użyciu szyfrowanego protokołu TLS 1.2. Moduły muszą umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem.

b) Dane, które dotyczą działań pracownika na komputerze, a więc: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., muszą być odseparowane od danych stricte technicznych tj. informacji o stacji roboczej. Muszą one być pogrupowane w osobnym, dedykowanym oknie. Musi to pozwalać na, zgodne z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej. Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, objęty jest kontrolą na poziomie wybranych Administratorów w programie można nadawać kontom administracyjnym różne poziomy dostępu oraz uprawnień zarówno do grup urządzeń, jak i użytkowników

c) Oprogramowanie musi być dostarczone z licencją bezterminową na co najmniej 96 dodatkowych urządzeń aktywnych dla których możliwa jest instalacja i konfiguracja agenta. Zamawiający obecnie posiada oprogramowanie Axence nVision Server oraz 30 licencji nVision axence dla wszystkich modułów. Dostawa musi zostać zrealizowana jako rozszerzenie istniejących/posiadanych przez Zamawiającego 30 licencji oprogramowania nVision axence lub 30 licencji oprogramowania kompatybilnego. Przez kompatybilność z istniejącym oprogramowaniem należy rozumieć możliwość centralnego zarządzania wszystkimi licencjami łącznie przy pomocy konsoli.

2. Monitorowanie infrastruktury:

a) Bezagentowo, musi obejmować serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:
   i) wykrywania urządzeń w sieci poprzez skanowanie ping (oraz arp-ping)
   ii) wizualizacji stanu urządzeń w postaci ikon urządzeń na mapach sieci,
   iii) wizualizacji połączeń pomiędzy urządzeniami a przełącznikami i informacji, do którego portu przełącznika podłączone jest dane urządzenie,
   iv) serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów,
   v) serwerów pocztowych:
      (1) program monitoruje zarówno serwis odbierający, jak i wysyłający pocztę,
      (2) program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem),
      (3) program ma możliwość wykonywania operacji testowych,
      (4) program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa,
   vi) monitorowania serwerów WWW i adresów URL,
   vii) obsługi szyfrowania TLS w powiadomieniach e mail,
   viii) obsługi urządzeń SNMP wspierających SNMP v1/2/3 (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP, temperatura, wilgotność, napięcie zasilania, itp.),
   ix) obsługi komunikatów syslog i pułapek SNMP,
   x) monitoringu routerów i przełączników wg:
      (1) zmian stanu interfejsów sieciowych,
      (2) ruchu sieciowego,
      (3) podłączonych stacji roboczych,
      (4) ruchu generowanego przez podłączone stacje robocze.
   xi) serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie;
   xii) wydajności systemów Windows obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy.

b) Oprogramowanie musi posiadać możliwość tworzenia dynamicznych map tworzonych wg. własnych filtrów, pozwalających na logiczną strukturę organizację zarządzania urządzeniami.

3. Inwentaryzacja infrastruktury:

a) Oprogramowanie musi automatycznie gromadzić informację o sprzęcie komputerowym i oprogramowaniu na komputerach oraz:
   i) prezentować szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.,
   ii) prezentować m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade,
   iii) informować o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji,
   iv) zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranym komputerze: instalacji/deinstalacji aplikacji, zmian adresu IP itd.,
   v) posiadać możliwość wysyłania powiadomienia np. e mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera,
   vi) umożliwiać odczytanie numeru seryjnego (klucze licencyjne),
   vii) umożliwiać automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych,
   viii) umożliwiać przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
b) Oprogramowanie inwentaryzacji sprzętu musi umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie:
   i) przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,
   ii) definiowania własnych typów (elementów wyposażenia), ich atrybutów oraz wartości dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer i skan faktury zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu i skan gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, inny dowolny załącznik (np. plik .DOCX, .XLSX, .PDF), skan dowolnego dokumentu, czy też własny komentarz; dodatkowo istnieje możliwość importu danych z zewnętrznego źródła (.CSV),
   iii) generowania zestawienia wszystkich środków trwałych, w tym urządzeń i zainstalowanego na nich oprogramowania:
   iv) archiwizacji i porównywania audytów środków trwałych,
   v) tworzenia kodów kreskowych w środkach trwałych,
   vi) drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla środków trwałych, które posiadają numer inwentarzowy,
   vii) inwentaryzacji sprzętu posiadającego kody kreskowe za pomocą aplikacji mobilnej na system Android,
   viii) inwentaryzacji komputerów niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline);
c) Dodatkowo muszą być dostępni agenci inwentaryzacji na systemy Android, macOS oraz Linux.
d) Inwentaryzacja oprogramowania musi zapewnić funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:
   i) skanowanie plików wykonywalnych i multimedialnych na komputerach, skanowanie archiwów ZIP,
   ii) zarządzanie posiadanymi licencjami,
   iii) łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych,
   iv) zarządzanie posiadanymi licencjami: raport zgodności licencji.
   v) możliwość przypisania do programów numerów seryjnych wartości itp.
e) Okna audytowe posiadają możliwość filtrowania elementów per oddział.

4. Obsługa użytkowników:

a) Oprogramowanie musi umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:
   i) faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),
   ii) procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach,

iii) rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona),
iv) informacji o edytowanych przez użytkownika dokumentach,
v) historii pracy (cykliczne zrzuty ekranowe),
vi) listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt),
vii) transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),
viii) wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem komputera (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program musi mieć możliwość monitorowania kosztów wydruków,
ix) nagłówków przesyłanej poczty e mail.

b) Oprogramowanie ponadto musi posiadać możliwość:
i) blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla danej stacji roboczej z możliwością definiowania wyjątków zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub domen (np. *.domena.pl),
ii) blokowania ruchu na wskazanych portach TCP/IP,
iii) blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,
iv) wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia.
v) generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie.
vi) blokowania uruchamiania aplikacji.
vii) tworzenia grup użytkowników do których można przypisywać określonych użytkowników

5. Zdalna pomoc użytkownikom:

a) Musi umożliwiać podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli. Podczas dostępu zdalnego, zarówno użytkownik jak i administrator widzą ten sam ekran. Administrator w trakcie zdalnego dostępu ma możliwość zablokowania działania myszy oraz klawiatury dla użytkownika. W niniejszym module musi znajdować się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych, które z kolei są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie.
b) Musi umożliwiać użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron.
c) Moduł musi zawierać komunikator (czat), który umożliwia przesyłanie wiadomości pomiędzy zalogowanymi użytkownikami i administratorami (wraz z wyszukiwarką wiadomości) oraz bazę wiedzy pomagającą użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy.:
d) Moduł pomocy zdalnej musi umożliwiać:
i) pobieranie listy użytkowników z Active Directory,
ii) przypisywanie pracowników helpdesk do kategorii zgłoszeń,
iii) procesowanie zgłoszeń użytkowników z wiadomości e mail,
iv) wykonywanie operacji na wielu zgłoszeniach równocześnie,
v) dołączanie załączników do zgłoszeń,
vi) zrzuty ekranowe (podgląd pulpitu),
vii) dystrybucję oprogramowania przez agenta,
viii) dystrybucję oraz uruchamianie plików za pomocą agentów (w tym plików MSI),
ix) zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku,
x) możliwość skonfigurowania automatyzacji procesowania zgłoszeń,
xi) planowanie nieobecności pracowników helpdesk,
xii) obsługę umów o gwarantowanym poziomie świadczenia usług (SLA),
xiii) generowanie raportów obsługi helpdesk,
xiv) zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu)

6. Ochrona przed wyciekiem danych:

a) Oprogramowanie musi umożliwiać blokowanie urządzeń w tym:
   i) blokowanie urządzeń i nośników danych, program ma możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny,
   ii) blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek,
   iii) blokowanie interfejsów bezprzewodowych: Wi Fi, Bluetooth, IrDA,
   iv) blokownie dotyczy tylko urządzeń służących do przenoszenia danych inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane.

b) Zarządzanie prawami dostępu do urządzeń:
   i) definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików;
   ii) autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. urządzenia prywatne są blokowane,
   iii) całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników,
   iv) centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.

c) Audyt operacji na urządzeniach przenośnych:
   i) zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.
   ii) podłączenie/odłączenie urządzenia przenośnego.

d) Integracja z Active Directory zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Przydzielanie uprawnień również do kont użytkowników lokalnych.

e) Program musi być zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora. Program musi być dostępny w języku polskim i angielskim wraz z podręcznikiem użytkownika w formie strony internetowej.

7. Monitorowanie temperatury i wilgotności powietrza w serwerowni głównej i zapasowej:

a) W ramach zamówienia Wykonawca musi dostarczyć i skonfigurować fizyczne urządzenia/czujniki współpracujące z dostarczonym oprogramowaniem do zarządzania, co najmniej po jednym dla serwerowni głównej i zapasowej, które będą umożliwiały odczytywanie aktualnej temperatury i wilgotności, a następnie tą informację przekazywały on-line do oprogramowania do zarządzania. Kolejno administrator będzie mógł ją odczytać na monitorze swojego komputera z poziomu oprogramowania do zarządzania.

IV. WYMAGANE ZAŁĄCZNIKI DO OFERTY

DOKUMENTUJĄCE ZGODNOŚĆ OFERTY Z WYMOGAMI TECHNICZNYMI DLA ELEMENTÓW INSTRASTRUKTURY SERWEROWEJ

W celu potwierdzenia, że oferowany przedmiot zamówienia odpowiada wymaganiom technicznym określonym przez Zamawiającego, Zamawiający wymaga dołączenia do oferty następujących załączników:

1) Wydruku wyników testów wydajności dla macierzy centralnej – przeprowadzonego zgodnie z wymaganiami SIWZ oddzielnie pomiaru wydajności w IOPS operacji zapisu i odczytu danych na pamięciach flash (SSD/NVMe) oraz wydajności w MB/s operacji zapisu i odczytu danych na dyskach magnetycznych (HDD) – potwierdzających, że zaoferowana (deklarowana) wydajność macierzy może być uzyskana w zaoferowanej konfiguracji macierzy; *Uwaga! wynik testu wydajnościowego nie musi być podany dla identycznej konfiguracji macierzy jak konfiguracja, która została zaoferowana, jednak konfiguracja ta musi być zbliżona do zaoferowanej macierzy pod względem liczby i rodzaju kontrolerów dyskowych, liczby i rodzaju napędów pamięci flash (SSD/NVMe) i napędów dyskowych (HDD) oraz liczby i rodzajów interfejsów sieciowych do serwerów (np. FC vs Ethernet);*
2) Kalkulacji pojemności użytkowej macierzy centralnej lub zrzutu ekranu z narzędzia do wyliczania pojemności macierzy dostarczonego przez producenta – potwierdzających, że zaoferowana (deklarowana) pojemność użytkowa macierzy centralnej może być uzyskana w zaoferowanej konfiguracji macierzy;
3) Kalkulacji pojemności użytkowej macierzy obiektowej lub zrzutu ekranu z narzędzia do wyliczania pojemności macierzy dostarczonego przez producenta – potwierdzających, że zaoferowana (deklarowana) pojemność użytkowa macierzy obiektowej może być uzyskana w zaoferowanej konfiguracji macierzy;
4) Kalkulacji pojemności użytkowej systemu wykonywania kopii zapasowych lub zrzutu ekranu z narzędzia do wyliczania pojemności (sizing) system wykonywania kopii zapasowych dostarczonego przez producenta tego systemu – potwierdzających, że zaoferowaną (deklarowaną) pojemność użytkową macierzy obiektowej może być uzyskana w zaoferowanej konfiguracji systemu wykonywania kopii zapasowych;
5) Schematów blokowych dostarczanych elementów infrastruktury serwerowej prezentujących – ideowo – sposób rozmieszczenia tych elementów w serwerowniach Biblioteki Śląskiej oraz połączenia logiczne między tymi elementami (lokalne i pomiędzy serwerowniami);
6) Schematów ideowych logicznych i fizycznych połączeń sieciowych dla sieci LAN i SAN – dla poszczególnych serwerowni Biblioteki Śląskiej
7) Schematów ideowych połączeń zasilających dostarczane elementów infrastruktury serwerowej – dla poszczególnych serwerowni Biblioteki Śląskiej
8) Schematów rozmieszczenia szaf i sprzętu w obu serwerowniach Biblioteki Śląskiej oraz instalacji sprzętu IT w szafach (wykazujących możliwość umieszczenia zaoferowanych szaf serwerowniach zgodnie z wymogami oraz instalacji elementów oferowanej infrastruktury serwerowej w dostarczanych szafach zgodnie ze zdefiniowanymi wymogami);