Załącznik nr 2
do Umowy

Opis Przedmiotu Zamówienia
na wdrożenie systemu zarządzania informacją o rezerwach strategicznych.

Spis Treści

1. Wstęp 4

2. Definicje 5

3. Techniczny Opis Przedmiotu Zamówienia 9

3.1. System Zarządzania Informacją o Rezerwach Strategicznych – Architektura 9

3.1.1. Architektura logiczna komponentów aplikacyjnych systemu SZIRS 9

3.1.2. Architektura fizyczna komponentów infrastrukturalnych systemu SZIRS 10

3.2. Wymagania minimalne dla poszczególnych komponentów infrastrukturalnych systemu SZIRS 12

3.2.1. Wymagania ogólne dla wszystkich komponentów sprzętowych 12

3.2.2. Wymagania funkcjonalne i techniczne dla Sprzętu 13

3.2.3. Wymagania funkcjonalne dotyczące modułu zarządzania serwerami rack 13

3.2.4. Wymagania funkcjonalne dotyczące integracji serwerów i macierzy z oprogramowaniem do zarządzania serwerami i macierzami. 15

3.2.5. Serwery Master Node – 3 szt. 16

3.2.6. Serwery Worker Node – 3 szt. 18

3.2.7. Macierze dyskowe All Flash– 1 szt. 20

3.2.8. Przełączniki SAN – 2 szt. 32

3.2.9. Przełączniki LAN 10\25 GbE – 2 szt. 33

3.2.10. Przełączniki LAN 1 GbE – 1 szt. 37

3.2.11. Platforma zarządzania kontenerami 43

3.2.11.1. Wstęp 43

3.2.11.2. Ogólna architektura aplikacyjnej platformy kontenerowej Kubernetes 44

3.2.11.3. Proponowana architektura pojedynczego klastra Kubernetes. 44

3.2.11.4. Architektura aplikacyjnej platformy kontenerowej Kubernetes dla dwóch ośrodków przetwarzania danych w ramach ewentualnej rozbudowy w przyszłości 45

3.2.11.5. Architektura wysoko-dostępna środowiska Kubernetes 45

3.2.11.6. Architektura rozwiązania CI/CD dla aplikacyjnej platformy kontenerowej Kubernetes 46
3.2.11.7. Rozwiązanie CI/CD dla platformy Kubernetes 46
3.2.11.8. Docelowa architektura dla aplikacyjnej platformy kontenerowej Kubernetes (rozwiązanie docelowe – po rozbudowie na dwa ośrodki przetwarzania oraz o środowisko Testowo-Rozwojowe na dedykowanym klastrze). 48
3.2.11.9. Opis docelowa architektury platformy aplikacji kontenerowych Kubernetes (rozwiązanie docelowe – po rozbudowie na dwa ośrodki przetwarzania oraz o środowisko Te-stowo-Rozwojowe na dedykowanym klastrze) 48
3.2.11.10. Wymagania funkcjonalne aplikacyjnej platformy kontenerowej Kubernetes 49
3.2.11.11. Wymagania funkcjonalne rejestru obrazów kontenerów:..... 57
3.2.11.12. Wymagania funkcjonalne modułu bezpieczeństwa kontenerów: 58
3.2.11.13. Wymagania funkcjonalne modułu zarządzania środowiskiem hybrydowym (wiele klastrów na wielu infrastrukturach):..... 59
3.2.11.14. Wymagania funkcjonalne modułu integracji platformy kontenerowej z rozwiązaniami obsługi zasobów dyskowych:..... 61
3.2.11.15. Wymagania funkcjonalne rozwiązania dyskowego zarządzanego programowo: 61
3.2.12. System backupu 63
3.2.12.1. Wstęp 63
3.2.12.2. Wymogi podstawowe oprogramowania backupowego 64
3.2.12.3. Wymogi dla licencjonowania (licencjonowanie typu perpertual) 79
3.2.12.4. Wymogi dla urządzeń wchodzących w skład systemu backupu 80
3.2.12.4.1. Ogólne 80
3.2.12.4.2. Wymagania dla serwera backupu – 1 szt. 81
3.2.12.4.3. Wymagania dla serwera proxy\media agent – 1 szt. 82
3.2.12.4.4. Wymagania dla macierzy backup – 1 szt. 84
3.3. Wymagania funkcjonalne dla Oprogramowania Dedykowanego systemu SZIRS 96
3.3.1. Opis Systemu 96
3.3.2. Podsystem Centralizacji Danych 96
3.3.3. Podsystem Wyszukiwania i Sprawozdawczości 97

3.3.4. Podsystem Wymiany Danych 97
4. Organizacyjny Opis Przedmiotu Zamówienia 97
4.1. Terminy Realizacji Przedmiotu Zamówienia 97
4.2. Wymagania w zakresie gwarancji 98
4.2.1. Wymagania ogólne 98
4.2.2. Warunki Gwarancji Sprzętu 101
4.2.3. Warunki Gwarancji dla Oprogramowania Standardowego 102
4.2.4. Poziomy SLA 103
4.3. Wymagania w zakresie dokumentacji projektowej 104
4.3.1. Wstęp 104
4.3.2. Projekt Wykonawczy wdrożenia dostarczanych elementów SZIRS 104
4.3.3. Dokumentacja Testowa 109
4.3.4. Plan Testów Akceptacyjnych 109
4.3.5. Scenariusze testowe 111
4.3.6. Dokumentacja Powykonawcza, która powstanie jako uaktualnienie Projektu Wykonawczego wdrożenia dostarczanych elementów SZIRS, ... 115
4.3.7. Procedury operacyjne i administracyjne 120
4.4. Wymagania w zakresie wdrożenia 120
4.4.1. Wymagania w zakresie dostawy: 120
4.4.2. Wymagania w zakresie Wdrożenia: 121
4.5. Wymagania w zakresie warsztatów 121
4.6. Wymagania co do osób realizujących zamówienie ze strony Wykonawcy 124

1. Wstęp

Celem realizacji projektu jest stworzenie centralnego systemu, skupiającego dane o rezerwach strategicznych zarządzanych przez Rządową Agencję Rezerw Strategicznych, pochodzące z obecnych systemów zarządzania rezerwami, w szczególności z systemów magazynowych oraz z systemów wdrożonych w jednostkach terenowych przez dysponentów takich rezerw. Budowa nowego systemu

ma być oparta na nowoczesnych rozwiązaniach sprzętowych oraz oprogramowaniu, w szczególności na mikrousługach posadowionych na platformie konteneryzacyjnej. Architektura systemu ma zapewniać wysoką dostępność w przypadku awarii poszczególnych elementów sprzętowych systemu w podstawowym ośrodku przetwarzania, jak również posiadać możliwość rozbudowy w przyszłości o drugi ośrodek przetwarzania w celu zabezpieczenia na wypadek wystąpienia katastrofy (Disaster Recovery).

Realizacja systemu jest podzielona na etapy:

1. Faza 1 - dostawa Sprzętu i Oprogramowania obejmującej serwery, macierze dyskowe, przełączniki SAN, przełączniki LAN, platformę zarządzania kontenerami oraz system backupu wraz z zapewnieniem gwarancji oraz usług serwisowych;
2. Faza 2 - instalacja, i konfiguracja sprzętu i oprogramowania wymienionego w pkt. 1;
3. Faza 3 - wdrożenie systemu zarządzania informacją o rezerwach strategicznych.

2. Definicje

Terminy lub zwroty, użyte w projektowanych postanowieniach Umowy, posiadają następujące znaczenie:

Termin	Definicja
API (Application Programming Interface)	Zbiór reguł ściśle opisujący sposób, w jaki programy lub podprogramy komunikują się ze sobą.
Deduplikacja danych	Eliminowanie powtarzających się części w zbiorze danych. Jest to proces stosowany przy zapisie danych, którego celem jest ograniczanie ilości miejsca potrzebnego do przechowywania danych.
Kompresja danych	Zmiana sposobu zapisu informacji tak w taki sposób aby zmniejszyć powtarzalność i tym samym objętość zbioru. Innymi słowy chodzi o wyrażenie tego samego zestawu informacji, lecz za pomocą mniejszej liczby bitów.
Failover/Failback	Failover - przełączenie na element zapasowy Systemu w momencie awarii elementu podstawowego. Failback - przełączenie na element podstawowy Systemu z systemu zapasowego po usunięciu awarii.

Klaster	Zbiór połączonych jednostek komputerowych (serwerów), które współpracują ze sobą w celu udostępnienia zintegrowanego środowiska umożliwiającego uzyskanie odpowiedniej: wydajności, niezawodności i równoważenia obciążenia.
Komponenty	Bloki funkcjonalne składające się na System, tj.: serwery, klastry, kopie zapasowe/archiwum, Oprogramowanie Standardowe oraz Oprogramowanie Dedykowane
Kopia migawkowa	Kopia pamięci dyskowej maszyny wirtualnej z określonego momentu czasu, umożliwiająca przywrócenie stanu maszyny wirtualnej na dany moment utworzenia kopii migawkowej; stan danych plikowych z momentu utworzenia migawki jest stały, niezmienny w czasie przez działającą maszynę wirtualną.
Węzeł / Kolokacja	Miejsce fizyczne, powierzchnia kolokacyjna, w którym pracuje węzeł sieci.
Platforma	Platforma kontenerowa – środowisko uruchomieniowe aplikacji kontenerowych - na potrzeby usługi Systemu Zarządzania Informacją o Rezerwach Strategicznych
SZIRS	System Zarządzania Informacją o Rezerwach Strategicznych
Plug-in	Inaczej „wtyczka”, dodatkowy moduł do programu komputerowego, który komunikuje się z nim poprzez interfejs API (Application Programming Interface), rozszerzając możliwości produktu wyjściowego.
Rozwiązanie	Całość współpracującego oprogramowania wymaganego do tworzenia i zarządzania klastrami platformy kontenerowej.
Szyfrowanie danych	Proces ukrywania danych w taki sposób, aby ich odczytanie możliwe było przez osoby posiadające „klucz” deszyfrujący
ThinProvisioning	Technologia wirtualizacji umożliwiająca przydzielenie większej ilości zasobów fizycznych niż są one faktycznie dostępne
ThickProvisioning	Technologia wirtualizacji umożliwiająca przydzielenie wymaganej ilości zasobów fizycznych zapewniając ich rezerwację i dostępność.
Administrator	Osoby wskazane przez Zamawiającego do kontaktu oraz bieżącej współpracy z Wykonawcą w ramach realizacji Umowy.
Usługi Serwisowe	Gwarantowana pomoc w eksploatacji (w tym rozwiązywaniu problemów (Błędów), wykonywania Napraw oraz Serwis Prewencyjny) Oprogramowania, udzielana Zamawiającemu przez producenta i/lub Wykonawcę.
Gwarancja	Gwarancja producenta na Sprzęt, Oprogramowanie Standardowe oraz Oprogramowanie Dedykowane

Czas naprawy	Czas liczony od następnego Dnia Roboczego od momentu przekazania przez Zamawiającego Zgłoszenia Błędu do momentu wykonania przez Wykonawcę Naprawy.
Czas reakcji	Czas mierzony od momentu przekazania przez Zamawiającego Zgłoszenia Błędu do momentu podjęcia działań przez Wykonawcę zmierzających do ustalenia przyczyn i usunięcia Błędu.
Dokumentacja	Projekt Techniczny, Dokumentacja Techniczna oraz aktualizacje do ww. dokumentów.
Dzień Roboczy	Dzień kalendarzowy od poniedziałku do piątku w godzinach 8-16, z wyłączeniem dni ustawowo wolnych od pracy w Polsce.
Naprawa	Działanie polegające na usunięciu Błędu poprzez wyeliminowanie przyczyn oraz skutków jego wystąpienia i przywróceniu do stanu prawidłowego działania Oprogramowania sprzed wystąpienia Błędu.
Oprogramowanie Standardowe	Oprogramowanie wraz z licencją stanowiące gotowy produkt dostępny na rynku dla wielu podmiotów w publicznej ofercie danego producenta. Oprogramowanie standardowe może być Oprogramowaniem standardowym - publicznym lub Oprogramowaniem standardowym - własnościowym.
Oprogramowanie Dedykowane / System Dedykowany	Komputerowy program użytkowy, stworzony specjalnie na potrzeby danej instytucji bądź osoby. Programowany jest w oparciu o indywidualne preferencje podmiotu zlecającego a jego funkcjonalności są dostosowane do własnych potrzeb Zamawiającego.
Oprogramowanie	Oprogramowanie Standardowe i Dedykowane
Strona	Zamawiający lub Wykonawca, w zależności od kontekstu.
Strony	Łącznie: Zamawiający i Wykonawca.
Serwisant	Osoba świadcząca w imieniu Wykonawcy usługi stanowiące przedmiot Umowy.
Serwis Prewencyjny	Okresowe działanie polegające na przeglądzie stanu pracy, Oprogramowania, sprawdzeniu i ewentualnej aktualizacji wersji oprogramowania, celem zminimalizowania prawdopodobieństwa wystąpienia Błędu.
Błąd	Każda nieprawidłowość w działaniu Oprogramowania.
Zgłoszenie	Przekazanie Wykonawcy informacji o wystąpieniu Błędu.
Zgłoszenie Serwisowe	Działanie polegające na przekazaniu informacji do Wykonawcy w celu podjęcia przez niego prac serwisowych w zakresie opisanym w formularzu Zgłoszenia Błędu, dokonane przez przedstawiciela Zamawiającego za pomocą e-mail lub portalu internetowego.

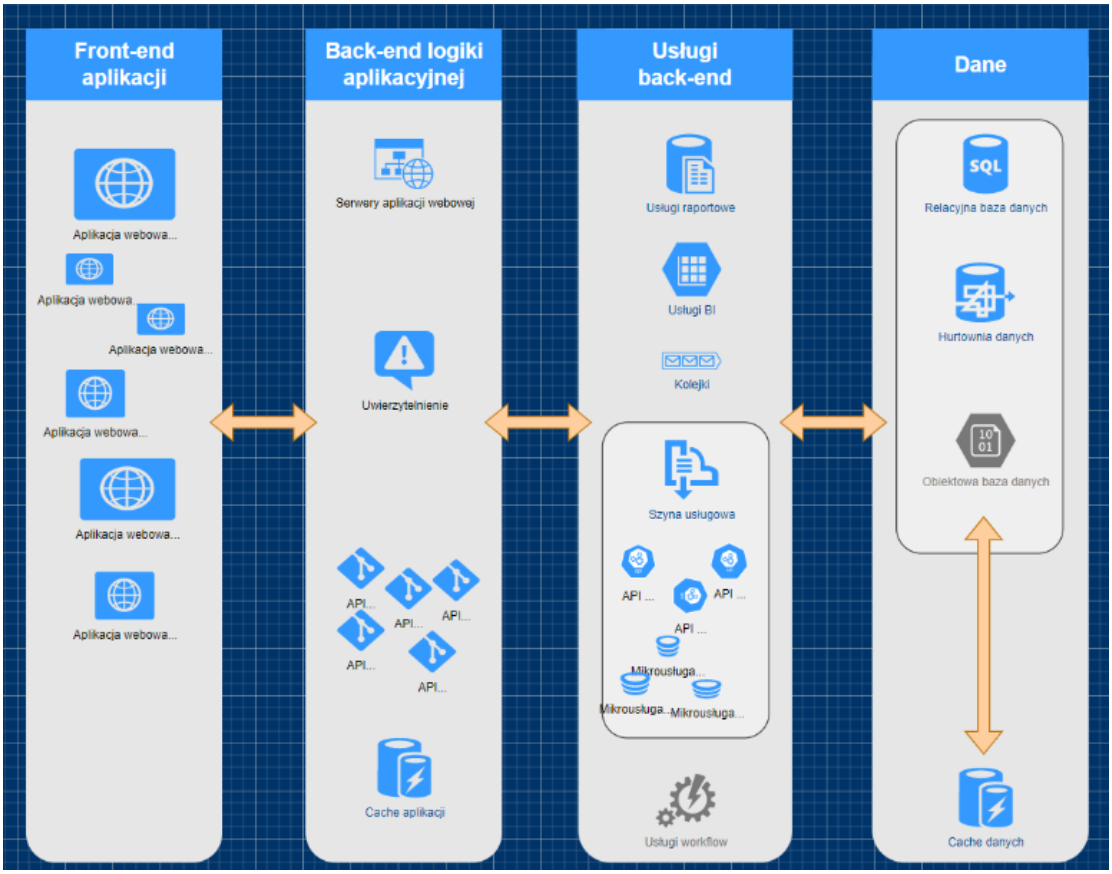
Błąd Krytyczny	Błąd uniemożliwiający pracę ze Sprzętem lub Oprogramowaniem charakteryzujący się następującymi problemami: • Sprzęt lub Oprogramowanie przestało działać, • Sprzęt lub Oprogramowanie spowodowało utratę lub uszkodzenie danych. • nie działają podstawowe funkcjonalności Sprzętu lub Oprogramowania
Błąd Poważny	Błąd mający istotny wpływ na działanie Sprzętu lub Oprogramowania oraz brak możliwości zastosowania obejścia, charakteryzujący się następującymi problemami: • restart usług • zdegradowana wydajność • nie działają poszczególne funkcjonalności Sprzętu lub Oprogramowania ale istnieje możliwość zalogowania się i wykonania podstawowych czynności
Błąd Drobny	Błąd mający niski wpływ na działanie Sprzętu lub Oprogramowania oraz istnieje możliwość zastosowania obejścia, charakteryzujący się następującymi problemami: • widoczny jest komunikat Błędu ale istnienie możliwość zastosowania obejścia problemu • minimalny wpływ na wydajność • minimalny wpływ na obsługę • pytania dotyczące funkcjonalności Sprzętu lub Oprogramowania lub jego konfiguracji podczas wdrożenia
Zapytanie	Zapytanie dotyczące problemu z obsługą Sprzętu lub Oprogramowania nie mający wpływu na dostępność funkcjonalności, charakteryzujący się następującymi cechami: • zapytania dotyczące obsługi Sprzętu lub Oprogramowania • wyjaśnienia dotyczące dokumentacji • zapytania dotyczące usprawnienia działania Sprzętu lub Oprogramowania

3. Techniczny Opis Przedmiotu Zamówienia

3.1. System Zarządzania Informacją o Rezerwach Strategicznych – Architektura

3.1.1. Architektura logiczna komponentów aplikacyjnych systemu SZIRS

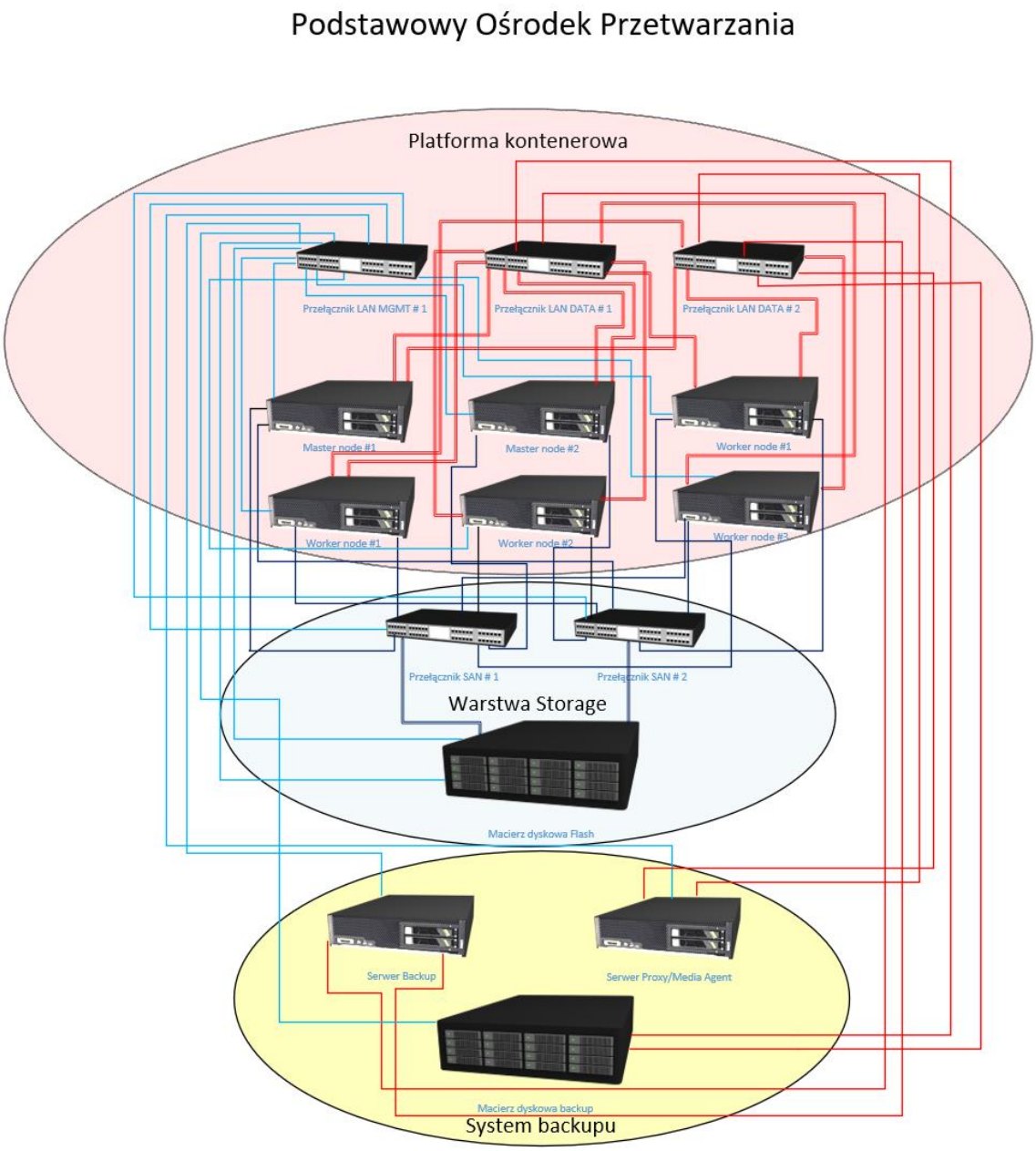
Poniższy rysunek prezentuje ogólny pogląd na architekturę systemu SZIRS z widokiem logicznym komponentów.



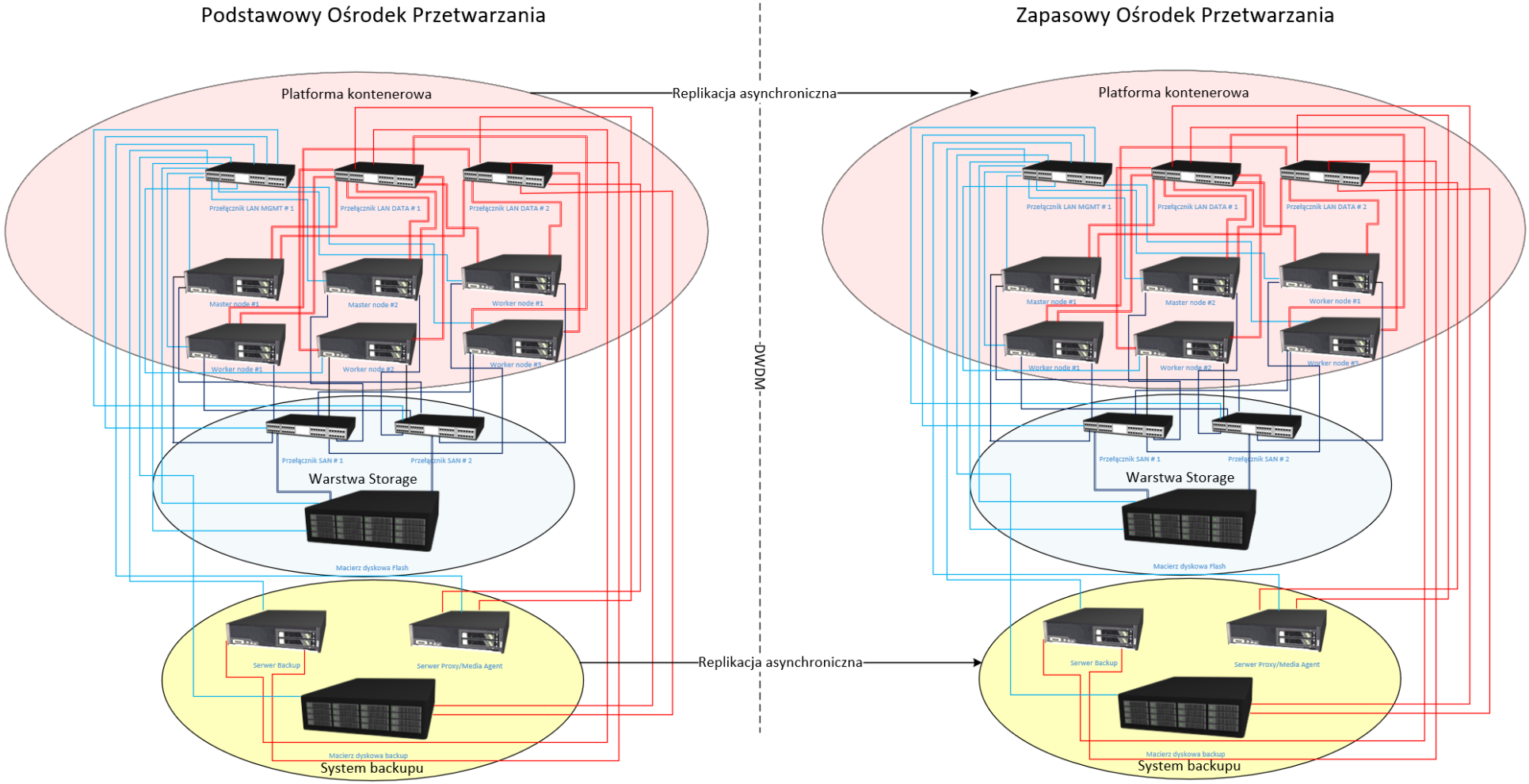
W obszarze FrontEnd aplikacji znajdują się komponenty odpowiedzialne za obsługę warstwy prezentacji. Przede wszystkim są to usługi dostarczające aplikacje webowe dla użytkowników. Obszar Backend logiki aplikacyjnej zawiera przede wszystkim usługi obsługujące logikę na potrzeby warstwy prezentacji wraz z warstwą cache (może być jako część Platformy) obsługująca wybrany ruch do obszaru Usług Backend. Z założenia usługi tej warstwy komunikują się jedynie bezpośrednio z warstwą usług Backend lub korzystają z systemów typu Szyna Usługowa lub Cache.
Środowisko uruchomieniowe, na którym System będzie posadowiony, ma być oparte na klastrach platformy kontenerowej służącej do uruchamiania aplikacji kontenerowych.
Kolorem szarym oznaczono komponenty rozwojowe, które nie są objęte niniejszym OPZ.

3.1.2. Architektura fizyczna komponentów infrastrukturalnych systemu SZIRS

Poniższy rysunek prezentuje ogólny pogląd na infrastrukturę systemu SZIRS z widokiem logicznym poszczególnych komponentów oraz ich połączeń w ramach pojedynczego ośrodka przetwarzania danych.



Poniższy rysunek prezentuje ogólny pogląd na infrastrukturę systemu SZIRS z widokiem logicznym poszczególnych komponentów oraz ich połączeń w ramach dwóch ośrodków przetwarzania danych. W ramach realizacji niniejszego projektu System będzie działał tylko w Podstawowym Ośrodku przetwarzania ale musi być przygotowany do ewentualnej rozbudowy w przyszłości o drugi ośrodek.



System SZIRS będzie posadowiony na platformie kontenerowej. Infrastruktura systemu będzie zlokalizowana w jednym ośrodku przetwarzania (podstawowym). Architektura Systemu musi pozwalać na rozbudowę w przyszłości o drugi ośrodek przetwarzania (zapasowy) dzięki czemu System będzie odporny na katastrofę. Dodatkowo Wykonawca zobowiązany jest dostarczyć i wdrożyć system backupu. Dane Systemu będą znajdowały się na dostarczonych macierzach dyskowych all flash, które będą połączone z serwerami za pośrednictwem sieci SAN. Komunikacja w sieci produkcyjnej LAN będzie oparta o przełączniki 10/25 GbE. Dodatkowo Wykonawca zobowiązany jest dostarczyć przełącznik LAN 1 GbE na potrzeby komunikacji z interfejsami zarządzającymi poszczególnych komponentów środowiska.

Zamawiający zapewni dodatkowo możliwość wykorzystania urządzeń równoważących ruch (Load Balancery).

Połączenia oznaczone kolorem niebieskim dotyczą sieci zarządzającej i oparte będą na linkach 1 GbE Ethernet.

Połączenia oznaczone kolorem czerwonym dotyczą sieci produkcyjnej oraz backupowej i oparte będą na linkach 25 GbE SFP28.

Połączenia oznaczone kolorem granatowym dotyczą sieci SAN i oparte będą na linkach 32 Gb FC SFP+ SW.

3.2. Wymagania minimalne dla poszczególnych komponentów infrastrukturalnych systemu SZIRS

3.2.1. Wymagania ogólne dla wszystkich komponentów sprzętowych

1. Każdy oferowany komponent musi być nieużywany i fabrycznie nowy, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez Producenta dla oferowanego modelu, pochodzić z oficjalnego kanału dystrybucji Producenta na rynek wewnętrzny Unii Europejskiej. Zamawiający nie dopuszcza oferowania komponentu będącego prototypem.
2. Poszczególne komponenty muszą pochodzić od producenta (muszą być kompletnym produktem opatrzonym numerem seryjnym producenta). Nie dopuszcza się komponentów opartych o elementy pochodzące od różnych producentów, które po zintegrowaniu proponowane są przez oferenta w ramach pojedynczego komponentu architektury. Wszystkie komponenty składowe muszą być identyczne dla wszystkich egzemplarzy danego sprzętu.
3. Oferowany sprzęt nie może być na liście produktów, dla których wsparcie Producenta zostanie zakończone w ciągu najbliższych 24 miesięcy.
4. Wraz z dostawą oferowanych komponentów Wykonawca musi dołączyć instrukcje obsługi pochodzące od producenta oferowanego komponentu w języku polskim lub angielskim w

formie papierowej lub elektronicznej (PDF, DOC). Zamawiający dopuszcza przekazanie linku do strony producenta na której opublikowane są dokumenty.

5. Wykonawca musi dostarczyć deklarację CE producenta dla oferowanego komponentu wraz z dostawą.
6. Gwarancja producenta na Sprzęt i Oprogramowanie Standardowe, nie może być krótsza niż 36 miesięcy, liczona od dnia podpisania Protokołu Odbioru Ilościowego
7. Urządzenia muszą być przystosowane do montażu w szafie stelażowej 19 cali i dostarczone wraz ze wszystkimi elementami niezbędnymi do ich zamontowania w szafie stelażowej.
8. Serwery muszą być produktami nowymi pochodzącymi od tego samego producenta z oficjalnego kanału partnerskiego – należy dostarczyć oświadczenie producenta.
9. Macierze muszą być produktami nowymi pochodzącymi od tego samego producenta z oficjalnego kanału partnerskiego – należy dostarczyć oświadczenie producenta.
10. Przełączniki muszą być zarządzane, konfigurowane, monitorowane przez posiadany przez Zamawiającego centralny system Cisco DNAC i dodane do konfiguracji w centralnie zarządzanym systemie Cisco ISE.

3.2.2. Wymagania funkcjonalne i techniczne dla Sprzętu

Wszystkie porty FC oraz LAN posiadające wymienne moduły SFP/SFP+/SFP28 itd. w każdym dostarczanym serwerze muszą być wyposażone we wkładki umożliwiające podłączenie do infrastruktury światłowodowej sieci LAN oraz SAN. Wkładki muszą zapewniać komunikację z prędkością określoną w wymaganiach.

Do każdego urządzenia należy dostarczyć patchcordy dla realizacji połączenia dedykowanego interfejsu zdalnego zarządzania oraz do połączeń LAN i SAN do przełączników.

Wszystkie procesory jak i rdzenie procesorowe zainstalowane w serwerze muszą być aktywne dla systemu operacyjnego oraz oprogramowania dodatkowego.

Wymaga się, aby oferowana konfiguracja była zgodna co do modelu serwera, modelu procesora, jego częstotliwości z konfiguracją serwera, dla której przeprowadzono test „SPECint_rate2017 Baseline” potwierdzony przez organizację SPEC (www.spec.org), na dzień podpisania umowy.

3.2.3. Wymagania funkcjonalne dotyczące modułu zarządzania serwerami rack.

Serwer musi być wyposażony w dedykowany moduł lub kartę zarządzającą będącą elementem fabrycznym serwera, zamontowaną w serwerze, posiadającą dedykowany port RJ-45 1

GbE, która udostępnia funkcjonalność zdalnego zarządzania serwerem, niezależnie od zainstalowanego na serwerze systemu operacyjnego (lub jego braku), posiadającą następujące funkcjonalności:

1. dostęp do modułu zarządzania serwerem z poziomu przeglądarki internetowej wspieranej przez system operacyjny Microsoft Windows 10/11,
2. włączenie, wyłączenie i restart serwera,
3. podgląd logów sprzętowych serwera i karty zarządzającej,
4. przejęcie zdalnej konsoli graficznej serwera i podłączanie wirtualnych napędów CD/DVD/ISO bez konieczności dokładania elementów sprzętowych,
5. zdalne, bezagentowe monitorowanie i informowanie o aktualnym statusie serwera i jego komponentów składowych:
    a) stan procesora,
    b) stan pamięci operacyjnej,
    c) stan kart rozszerzeń,
    d) stan komponentów tworzących pamięć masową,
    e) stan kontrolera RAID,
    f) stan karty sieciowej,
    g) stan karty FC,
    h) stan zasilacza,
    i) stan wentylatorów tworzących system chłodzenia serwera,

    Informacja o aktualnym statusie dotyczy komponentów zainstalowanych w serwerze. Informowanie o aktualnym statusie i nieprawidłowościach musi być realizowane w sposób jednoznaczny i wskazywać dokładny komponent, którego dotyczy.
6. zdalne monitorowanie w czasie rzeczywistym poboru prądu przez serwer i prędkości obrotowej wentylatorów,
7. zdalna inwentaryzacja serwera oraz jego wyposażenia składowego:
    a) model procesora,
    b) model i ilość modułów składających się na pamięć operacyjną serwera,
    c) gniazda rozszerzeń,
    d) komponenty tworzące pamięć masową,
    e) typ/model kontrolera RAID,
    f) typ/model karty sieciowej,
    g) typ/model karty FC,
    h) typ/PN/model zasilacza,
    i) wentylatory tworzące system chłodzenia serwera,

    Informacja o specyfikacji dotyczy komponentów zainstalowanych w serwerze. Cechy identyfikacyjne takie jak typ. model, numer seryjny muszą być jednoznacznie powiązane z komponentem, którego dotyczą.

8. szyfrowane połączenie (SSLv3 i/lub TLS) oraz uwierzytelnianie i autoryzację użytkownika,
9. integracja z usługą katalogową MS Active Directory w zakresie wykorzystania użytkowników logujących się do modułu zarządzania serwerem,
10. obsługę przez co najmniej dwóch zalogowanych administratorów jednocześnie,
11. wysyłanie do administratora maila z powiadomieniem o awarii,
12. obsługa protokołu SNMP do informowania o statusie serwera

3.2.4. Wymagania funkcjonalne dotyczące integracji serwerów i macierzy z oprogramowaniem do zarządzania serwerami i macierzami.

Zamawiający wymaga dostarczenia, zainstalowania i skonfigurowania oprogramowania Producenta do zarządzania serwerami i macierzami dla dostarczanych serwerów oraz macierzy wraz z niezbędnymi licencjami do zarządzania wszystkimi dostarczonymi serwerami. Oprogramowanie musi być dostarczone i zainstalowane w ramach pojedynczej instancji (jednej maszyny wirtualnej lub dodatkowego serwera fizycznego dostarczonego przez Wykonawcę) wraz ze wszystkimi licencjami na oprogramowanie niezbędne do uruchomienia Oprogramowania do zarządzania serwerami i macierzami (bez dodatkowych kosztów).

Oferowane Oprogramowanie musi zapewniać co najmniej następujące funkcjonalności w zakresie serwerów:

1. bezagentowe monitorowanie aktualnego stanu serwera i jego komponentów składowych z dokładnością do pojedynczego komponentu:
    a. stan procesora,
    b. stan pamięci operacyjnej serwera,
    c. stan komponentów tworzących pamięć masową,
    d. stan kontrolera RAID,
    e. stan karty sieciowej,
    f. stan karty FC,

   Informacja o aktualnym stanie dotyczy komponentów zainstalowanych w serwerze. Informowanie o aktualnym statusie i nieprawidłowościach musi być realizowane w sposób jednoznaczny i wskazywać dokładnie komponent, którego dotyczy.
2. wykrywanie i komunikacja z kartą zdalnego zarządzania serwerem,
3. inwentaryzację serwera – informacja o konfiguracji serwera i jego elementów składowych zawierającej co najmniej:
    a. numer seryjny,
    b. model procesora,
    c. model i ilość modułów składających się na pamięć operacyjną serwera,
    d. komponenty tworzące pamięć masową,
    e. typ/model kontrolera RAID,

f. typ/model karty sieciowej,
g. typ/model karty FC,

Informacja o specyfikacji dotyczy komponentów zainstalowanych w serwerze. Cechy identyfikacyjne takie jak typ, model, numer seryjny muszą być jednoznacznie powiązane z komponentem, którego dotyczą.

4. zarządzanie wieloma serwerami z jednej konsoli z podziałem na grupy, realizowane bez udziału dedykowanego agenta,
5. integracja z usługą katalogową MS Active Directory w zakresie wykorzystania użytkowników logujących się do oprogramowania do zarządzania serwerami,
6. równoczesne zarządzanie wieloma alarmami na serwerach,
7. zarządzanie i aktualizację oprogramowania firmware serwera dla wielu serwerów,
8. możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram lub automatyczne wykrywanie serwerów po ich podłączeniu do infrastruktury,
9. możliwość eksportu raportu co najmniej do CSV lub HTML lub XLS,
10. widok umożliwiający szybki podgląd stanu środowiska,
11. generowanie alarmów przy zmianie stanu monitorowanych komponentów, będących częścią składową serwera ze wskazaniem na konkretny komponent, z czasem reakcji nie dłuższym niż 5 min. od zaistnienia zdarzenia,
12. filtry raportów umożliwiające podgląd najważniejszych zdarzeń,
13. przejęcie zdalnej konsoli graficznej serwera i podłączanie wirtualnych napędów CD/DVD/ISO bez konieczności dokładania elementów sprzętowych,
14. możliwość definiowania ról administratorów,
15. możliwość zdalnej aktualizacji oprogramowania firmware dla pojedynczego elementu/komponentu wyposażenia serwera,
16. możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów,
17. przywracanie ustawień serwera (konfiguracji BIOS, wersji firmware) inicjowane przez Administratora, na podstawie danych zapisanych na karcie zarządzającej serwera lub w profilu serwera zdefiniowanym w oprogramowaniu zarządzającym serwerami.

3.2.5. Serwery Master Node – 3 szt.

Lp.	Element/cecha/komponent	Wymagania minimalne
1	Obudowa	Wysokość maksymalnie 1U, przystosowana do montażu w szafie stelażowej 19 cali (wraz ze wszystkimi elementami niezbędnymi do zamontowania serwera w szafie stelażowej

		z możliwością wysunięcia bez konieczności odłączania okablowania).
2	Procesor	Minimalna częstotliwość bazowa rdzeni procesorów zamontowanych w serwerze to 2,5 GHz, minimalna sumaryczna ilość rdzeni procesorów zamontowanych w serwerze to 32 szt. Procesory osiągające w testach „SPECint_rate2017 Baseline" wynik nie gorszy niż 350 pkt. Wynik testu musi dotyczyć oferowanego serwera.
3	Pamięć operacyjna	Minimum 256 GB DDR5 z ochroną pamięci ECC. Pamięci w oferowanej konfiguracji muszą pracować z szybkością transmisji danych nie niższą niż 4800MHz. Użyte kości pamięci muszą być jednakowe (model, rozmiar, typ). Serwer musi posiadać min. 32 gniazda pamięci RAM DDR5.
4	Gniazda rozszerzeń	Łącznie minimum 4 gniazda PCI Express w tym minimum 3 gniazda piątej generacji i minimum jedno gniazdo czwartej generacji. Minimum 1 gniazdo OCP 3.0
5	Dysk twardy	Serwer musi być wyposażony w minimum 2 szt. dysków SSD 240 GB, 2,5" SAS/SATA/U.2 Hot Plug, Read Intensive zamontowane w wewnętrznych kieszeniach serwera. Serwer musi być wyposażony w kontroler sprzętowy. zapewniający RAID 1 dla ww. dysków. Serwer musi zapewniać możliwość rozbudowy do minimum 4 szt. dysków (bez konieczności dokładania dodatkowych elementów). Wszystkie urządzenia muszą być zamontowane wewnątrz obudowy serwera, kompatybilne z systemem wirtualizacji dostarczanym w ramach niniejszego zamówienia.
6	Karty sieciowe	Minimum 4 szt. portów pracujących z minimalną prędkością 25 GbE, wyposażonych we wkładki SFP28.
7	Karty FC	Minimum 2 szt. portów pracujących z minimalną prędkością 32 Gb FC, wyposażonych we wkładki FC SW SFP+, obsługiwanych przez co najmniej dwie niezależne karty PCIe.
8	Karta graficzna	Zintegrowana karta graficzna do obsługi wyjścia wideo
9	Porty	Minimum 1 dodatkowy port RJ-45 dedykowany dla interfejsu zdalnego zarządzania, minimum 2 x USB zewnętrzne.

		Nie dopuszcza się stosowania spliterów oraz kart zajmujących wolne sloty PCIe w serwerze w celu osiągnięcia wymaganej liczby portów USB; minimum 1x VGA.
10	Zasilacz	Minimum dwa zasilacze wyposażone w złącza C13 hotplug, zapewniające redundancję zasilania na poziomie N+N. Połowa spośród zainstalowanych zasilaczy musi zapewniać możliwość zasilenia serwera, przy zachowaniu jego pełnych możliwości operacyjnych umożliwiających pracę z maksymalną wydajnością podczas pracy ciągłej.
11	Chłodzenie	Zestaw wentylatorów zapewniających redundantne chłodzenie serwera, typu hot-plug. Serwer musi zapewnić stabilne działanie przy temperaturze otoczenia co najmniej 25 st. C.
12	Wspierane systemy operacyjne i wirtualizacyjne	MS Windows Server 2022 lub nowsze wersje Red Hat Enterprise Linux 8.X lub nowsze wersje, VMware ESX 7.x lub nowsze wersje lub równoważne
13	Instalacja	Instalacja i konfiguracja serwera wykonana przez inżyniera producenta serwera

3.2.6. Serwery Worker Node – 3 szt.

Lp.	Element/cecha/komponent	Wymagania minimalne
1	Obudowa	Wysokość maksymalnie 2U, przystosowana do montażu w szafie stelażowej 19 cali (wraz ze wszystkimi elementami niezbędnymi do zamontowania serwera w szafie stelażowej z możliwością wysunięcia bez konieczności odłączania okablowania).
2	Procesor	Minimalna częstotliwość bazowa rdzeni procesorów zamontowanych w serwerze to 3.1 GHz, minimalna ilość procesorów to 2, minimalna sumaryczna ilość rdzeni procesorów zamontowanych w serwerze to 128 szt. Procesory osiągające w testach „SPECint_rate2017 Baseline” wynik nie gorszy niż 1290 pkt. Wynik testu musi dotyczyć oferowanego serwera.
3	Pamięć operacyjna	Minimum 512 GB DDR5 z ochroną pamięci ECC. Pamięci w oferowanej konfiguracji muszą pracować z szybkością

		transmisji danych nie niższą niż 4800MHz. Użyte kości pamięci muszą być jednakowe (model, rozmiar, typ). Serwer musi posiadać min. 20 gniazd pamięci RAM DDR5.
4	Gniazda rozszerzeń	Łącznie minimum 10 szt. gniazd PCI Express (w tym min 4 x16 i 4 x8 piątej generacji). Minimum 1 gniazdo OCP 3.0
5	Dysk twardy	Serwer musi być wyposażony w minimum 2 szt. dysków SSD 240 GB, 2,5" SAS/SATA/U.2 Hot Plug, Read Intensive zamontowane w wewnętrznych kieszeniach serwera. Serwer musi być wyposażony w kontroler sprzętowy, zapewniający RAID 1 dla ww. dysków. Serwer musi zapewniać możliwość rozbudowy do minimum 16 szt. dysków (bez konieczności dokładania dodatkowych elementów). Wszystkie urządzenia muszą być zamontowane wewnątrz obudowy serwera, kompatybilne z systemem wirtualizacji dostarczanym w ramach niniejszego zamówienia.
6	Karty sieciowe	Minimum 4 szt. portów pracujących z minimalną prędkością 25 GbE, wyposażonych we wkładki SFP28 obsługiwanych przez co najmniej dwie niezależne karty PCIe.
7	Karty FC	Minimum 4 szt. portów pracujących z minimalną prędkością 32 Gb FC, wyposażonych we wkładki FC SW SFP+, obsługiwanych przez co najmniej dwie niezależne karty PCIe.
8	Karta graficzna	Zintegrowana karta graficzna do obsługi wyjścia wideo
9	Porty	Minimum 1 dodatkowy port RJ-45 dedykowany dla interfejsu zdalnego zarządzania, minimum 3 x USB z czego 2 szt. w standardzie USB 3.1, zewnętrzne. Nie dopuszcza się stosowania spliterów oraz kart zajmujących wolne sloty PCIe w serwerze w celu osiągnięcia wymaganej liczby portów USB; minimum 1x VGA.
10	Zasilacz	Minimum dwa zasilacze wyposażone w złącza C19 hotplug, zapewniające redundancję zasilania na poziomie N+1 lub N+N. Każdy z zainstalowanych zasilaczy musi zapewniać możliwość zasilenia serwera, przy zachowaniu jego pełnych możliwości operacyjnych umożliwiających pracę z maksymalną wydajnością podczas pracy ciągłej.

11	Chłodzenie	Zestaw wentylatorów zapewniających redundantne chłodzenie serwera, typu hot-plug. Serwer musi zapewnić stabilne działanie przy temperaturze otoczenia co najmniej 25 st. C.
12	Wspierane systemy operacyjne i wirtualizacyjne	MS Windows Server 2022 lub nowsze wersje Red Hat Enterprise Linux 8.X lub nowsze wersje, VMware ESX 7.x lub nowsze wersje lub równoważne

3.2.7. Macierze dyskowe All Flash– 1 szt.

Lp.	Element/cecha/komponent	Wymagania minimalne
1	Dokumentacja producenta	Każda funkcjonalność wyspecyfikowana w dokumencie musi mieć potwierdzenie w aktualnym oraz ogólnodostępnym dokumencie producenta w postaci instrukcji użytkownika lub dokumentacji technicznej. W razie wątpliwości co do realizacji funkcjonalności, Zamawiający może zwrócić się do oferenta o udostępnienie wyżej wymienionych dokumentów w celu potwierdzenia jej realizacji.
2	Standard RACK	Wymagane jest rozwiązanie mieszczące się w standardowej, pojedynczej szafie 19” 42U, niededykowanej wyłącznie dla macierzy. Preferowane jest rozwiązanie kompaktowe tj., o jak najmniejszym rozmiarze fizycznym i charakteryzujące się niskim poborem energii wynoszącym nie więcej niż 1200W
3	Dostępność	Macierz klasy Enterprise pracująca w trybie symetric Active-Active (nie ALUA) co oznacza iż w przypadku utylizacji na poziomie 100% zapewnia: - uzyskanie wysokiej dostępności na poziomie 99.9999% dla pojedynczej macierzy. - braku spadku wymaganej wydajności macierzy w przypadku awarii połowy kontrolerów - braku spadku wymaganej wydajności w przypadku awarii dwóch dysków z tej samej pooli RAID - 100% odczytu z pełnej pojemności
4	Niezawodność	Rozwiązanie musi oferować dostępność na poziomie minimum 99,9999% lub wyższym w obrębie pojedynczej macie-

		rzy. Potwierdzenie realizacji tej funkcjonalności musi znajdować się w oficjalnej dokumentacji producenta oferowanego sprzętu. Architektura rozwiązania nie może mieć pojedynczego punktu awarii (SPOF). Dane musza być dostępne w przypadkach: - awarii jednej linii zasilania, - awarii dowolnego kontrolera, - awarii dowolnych dwóch nośników danych użytkownika, - awarii dowolnego portu FC/iSCSI, - awarii dowolnego modułu pamięci RAM lub dowolnego procesora kontrolera. Awaria i niedostępność pojedynczego kontrolera macierzy nie może powodować spadku wydajności całego rozwiązania – brak efektu tzw. „Degraded Performance failover". Oznacza to iż macierz musi posiadać identyczną wydajność w obydwu stanach: awarii oraz barku awarii. Zmiana wersji oprogramowania zarządzającego rozwiązaniem lub oprogramowania wbudowanego w kontrolery rozwiązania nie może powodować utraty dostępu do danych. Rozwiązanie nie może zawierać komponentów zapasowych, które nie są wykorzystywane podczas pracy urządzenia (np. zapasowy kontroler, dysk hot spare). Oferowana macierz musi gwarantować optymalizację inwestycji poprzez ciągłe wykorzystanie wszystkich elementów dostarczanego sprzętu. Rozwiązanie musi umożliwiać wymianę na gorąco (bez zatrzymywania dostępu do danych) następujących komponentów: kontrolerów, zasilaczy, wentylatorów, portów front-end i back-end, nośników NVME. Rozwiązanie musi umożliwiać bezpieczne wyłączenie urządzenia niepowodujące utraty danych użytkownika. Dane przechowywane w pamięci urządzenia muszą zostać trwale zapisane na nośniki Flash przed całkowitym wyłączeniem macierzy na skutek awarii bądź interwencji manualnej.
5	Obsługa komunikacji do hosta	Rozwiązanie musi być zbudowane w oparciu o dwa lub wielokrotność dwóch kontrolerów macierzowych pracujących

		symetrycznie w trybie active-active w zakresie obsługi danych wejściowych i wyjściowych. Tryb active-active jest wymagany niezależnie od liczby kontrolerów w macierzy. Macierz z włączonym trybem active-active nie może ograniczać wymaganej wydajności, pojemności oraz funkcjonalności (np. ilości wspieranych snapshotów). Niedopuszczalne są rozwiązania dual-active oraz ALUA (Asymmetric Logical Unit Access). Ze względu na specyfikę protokołu NVMe wymagane jest, aby połączenia pomiędzy wszystkimi kontrolerami macierzowymi były realizowane poprzez magistrale PCIe, dla konfiguracji: - dwu-kontrolerowej - cztero-kontrolerowej (warunek ten musi być spełniony nawet w przypadku, gdy opcja ta występuje jako element rozbudowy).
6	Architektura dostępu do danych	Macierz musi korzystać z globalnej puli nośników i danych niezależnie od wykorzystywanego kontrolera. Niedopuszczalne jest rozwiązanie, w którym LUNy bądź urządzenia fizyczne typu dysk/moduł są przypisywane do kontrolera. Rozwiązanie musi wspierać pracę na wszystkich portach front-end w trybie round-robin z niezmiennymi czasami odpowiedzi, niezależnie od aktualnie wykorzystywanego portu, kontrolera i wolumenu. Niedopuszczalne jest rozwiązanie typu ALUA.
7	Wydajność	Minimalna wymagana wydajność rozwiązania musi być osiągalna z aktywnymi i pracującymi wszystkimi funkcjami redukcji danych, niezależnie od stopnia zapełnienia przestrzeni fizycznej danymi tj. od zajętości 1 do 100%. Jeżeli macierz w obrębie dwóch kontrolerów nie jest w stanie utrzymać 100% wydajności, wymagane jest dostarczenie konfiguracji cztero-kontrolerowej zapewniającej ww. wydajność Niezależnie od rodzaju zapisanych danych i przy macierzy zapełnionej w przynajmniej 70% fizycznej pojemności, rozwiązanie w oferowanej konfiguracji musi oferować następującą wydajność na całej powierzchni dostępnej dla użytkownika, z aktywnymi i pracującymi wszelkimi oferowanymi

		funkcjami redukcji danych (thin-provisioning, deduplikacja, kompresja): - co najmniej 200 000 losowych operacji odczytu wykonywanych blokiem 8 kB ze średnim czasem odpowiedzi mierzonym po stronie hosta nieprzekraczającym 0.7 ms, - co najmniej 180 000 losowych operacji Zapisu wykonywanych blokiem 8 kB ze średnim czasem odpowiedzi mierzonym po stronie hosta nieprzekraczającym 0.7 ms, - co najmniej 160 000 losowych operacji odczytu/zapisu Read 50%/Write 50%wykonywanych blokiem 8 kB ze średnim czasem odpowiedzi mierzonym po stronie hosta nieprzekraczającym 0.7 ms, Te same parametry wydajnościowe muszą być spełnione w przypadku, gdy w czasie testów trwających minimum 60 minut, na wolumenach poddanych obciążeniu: - tworzone są kopie migawkowe - dane są dodawane i usuwane - z macierzy tymczasowo usunięte zostają minimum dwa nośniki Flash Zamawiający zastrzega sobie prawo do wykonania ww. testów wydajnościowych na etapie wdrożenia z wykorzystaniem oprogramowania Vdbench.
8	Skalowalność macierzy	Macierzy musi umożliwiać skalowalność wertykalną (scale-up) to jest taką gdzie konfiguracja inicjalna zaczyna się od niepełnego obsadzenia dyskami i pozwala na instalowanie kolejnych dysków w wolnych slotach półki oraz o dodatkowe półki bez wpływu na dostępność do danych, oraz bezprzerwową aktualizację do wyższego modelu macierzy.
9	Skalowalność kontrolerów	Rozbudowa macierzy musi być wykonywana na gorąco, bez konieczności migrowania danych na inne urządzenia i bezprzerwowo dla działania aplikacji korzystających z rozbudowywanej macierzy.
10	Bezprzerwowy upgrade kontrolerów	Oferowana macierz musi umożliwiać bezprzerwowe przejście do wyższego modelu macierzy tego samego producenta poprzez np. wymianę kontrolerów lub poprzez dołożenie dodatkowych kontrolerów, które będą tworzyły z oferowanymi w postępowaniu kontrolerami jeden spójny sys-

		tem macierzowy zarządzany z jednej konsoli administracyjnej. Wymiana kontrolerów lub ich dołożenie nie może powodować przerwy w dostępie do danych oraz utraty którejkolwiek z wymaganych funkcjonalności.
11	Skalowalność portów	Macierz musi posiadać (bez stosowania dodatkowych przełączników lub koncentratorów) możliwość skalowalności do minimum 20 portów Fibre Channel 32 Gbps lub 16 portów iSCSI 10 Gbps SFP+ w obrębie dwóch kontrolerów,
12	Pojemność	Oferowana macierz musi składać się z minimum 20 nośników Flash NVMe nie mniejszych niż 2 TiB (tebibytes) każdy oraz być rozbudowywalna do minimum 48 nośników flash. Macierz w oferowanej konfiguracji musi zapewniać minimum 26 TiB gwarantowanej przestrzeni użytkowej bez uwzględnienia wszelkich efektywności upakowania i redukcji danych. Macierz w oferowanej konfiguracji musi zapewniać minimum 80 TiB gwarantowanej przestrzeni efektywnej z uwzględnieniem wszelkich efektywności upakowania i redukcji danych. Macierz musi umożliwiać rozbudowę do co najmniej 150 TiB efektywnej przestrzeni w ramach pojedynczej obudowy. Zapełnienie macierzy w 100% dostępnej pojemności nie może powodować utraty dostępu do danych.
13	Kompatybilność z - (NVMe)	Macierz musi wykorzystywać protokół NVMe do wszystkich operacji wewnętrznych jak i komunikacji z dodatkowymi półkami dyskowymi niezależnie od skali oferowanego systemu. Niedopuszczalne jest stosowanie protokołów typu SAS bądź FC w żadnym wewnętrznym komponencie rozwiązania. Wykluczone jest tym samym stosowanie translacji kodowania NVMe do SAS pomiędzy różnymi komponentami macierzy. Macierz musi być wyposażona w procesory wyposażone we wsparcie dla protokołu NVME. Zamawiający dopuszcza architekturę X86 dwóch producentów procesorów Intel (z generacją co najmniej Skylake) oraz AMD (z generacją Epyc)

14	Bezpieczeństwo danych	Rozwiązanie musi szyfrować wszelkie przechowywane dane minimum algorytmem AES-256 lub silniejszym oraz szyfrować wszystkie nośniki flash obsługiwane w urządzeniu. Szyfrowanie danych nie może mieć wpływu na wydajność rozwiązania. Zgodnym z certyfikacją FIPS 140-2. Algorytm szyfrowania musi posiadać możliwość przechowywania klucza szyfrującego w: - Serwerze kluczy zgodnym ze standardem KMIP - kartach SmartCard podłaczonych poprzez czytniki do portów USB macierzy. - systemie macierzowym - wsparcie dla kluczy Yubikey Klucz szyfrujący musi być domyślnie przechowywany na macierzy i generowany w sposób uniemożliwiający odczyt danych z usuniętych z macierzy nośników Flash. Szyfrowanie musi być rozwiązaniem niezależnym od producenta modułów Flash w pełni kontrolowanym przez producenta macierzy.
15	Ochrona nośników danych	W celu zapewnienia ochrony danych każdy dysk oraz moduł w macierzy musi przechowywać w tym samym momencie dane parzystości, dane aplikacji oraz przestrzeń zapasową. Ochrona danych musi być realizowana za pomocą tzw. rozproszonej podwójnej parzystości na poziomie blokowym. Niedopuszczalne są klasyczne realizacje ochrony danych oparte grupy dysków w RAID 4/5/6 oraz RAID 10. W szczególności niedopuszczalne jest stosowanie dedykowanych dysków parzystości tzw. parity drives oraz dedykowanych dysków zapasowych tzw. hot spare drives. Niedopuszczalne jest stosowanie dysków dedykowanych tylko do konkretnych typów danych. Zaoferowane nośniki flash NVMe muszą wspierać, wszystkie typy RAID obsługiwane przez oferowany system macierzowy.
16		Rozwiązanie musi oferować mechanizm monitorowania trwałości nośników Flash i realizować funkcję proaktywnej

		odbudowy czyli zgłoszenia awarii nośnika jeszcze zanim jego komórki ulegną całkowitemu wypaleniu. Rozwiązanie musi oferować mechanizm weryfikacji odczytywanych danych, wykrywania i naprawiania uszkodzonych danych w sposób przezroczysty dla hosta. Rozwiązanie musi być odporne na jednoczesną awarię minimum dwóch dowolnych nośników Flash, niezależnie od skali i konfiguracji rozwiązania. W przypadku awarii dwóch nośników macierz musi zapewnić bezprzerwowy dostęp do wszystkich danych na macierzy.
17	Połączenia do hostów oraz replikacji - wymaganie globalne	Niedopuszczalne jest stosowanie sprzętu pośredniczącego oraz niedopuszczalne jest wykorzystywanie ww. portów FCP do komunikacji z hostami. Niedopuszczalne jest wykorzystywanie portów FC oraz SAS do łączenia kontrolerów macierzowych. Zastosowane karty FC muszą obsługiwać protokół NVMe-o-F (NVMe over Fabrics). Zmiana wykorzystywanego przez karty protokołu pomiędzy FC a NVMe-o-F musi być możliwa dla administratora oraz odbywać się bezprzerwowo z punktu widzenia dostępu do danych. Zabronione jest emulowanie protokołów blokowych takich jak FCP oraz iSCSI, macierz musi natywnie bez warstw pośredniczących wspierać powyższe protokoły.
18	Porty ETHERNET	Rozwiązanie musi posiadać natywne podłączenie do hostów poprzez protokół iSCSI zapewniając minimalną ilość 4 portów 10 Gbit/s SFP+ Ethernet (min 2 per kontroler). Niedopuszczalne jest stosowanie sprzętu pośredniczącego iSCSI-FC itp. Zmiana przepustowości portu 10Gbit/s na 25Gbit/s musi być możliwa poprzez wymianę modułu SFP+ a nie całej karty HBA w kontrolerze.
19	Porty FC (HBA)	Rozwiązanie musi posiadać natywne podłączenie do hostów poprzez protokół FC zapewniając minimalną ilość 4 portów 32 Gb SFP+ (min 2 per kontroler). Niedopuszczalne jest stosowanie sprzętu pośredniczącego iSCSI-FC itp. Zmiana przepustowości portu 32Gbit/s na 16Gbit/s musi być możliwa poprzez wymianę modułu SFP+ a nie całej karty HBA w kontrolerze.

20	Porty do zarządzania	Każdy kontroler musi posiadać 2 porty RJ45 każdy 1Gbit/s Ethernet przeznaczone do zarządzania. System musi wspierać możliwość zarządzania portami dedykowanymi do replikacji lub ruchu iSCSI.
21	Funkcje redukcji i prezentacji danych	Rozwiązanie musi realizować funkcję thin-provisioningu dla wszystkich udostępnianych wolumenów oraz dostarczenie funkcji space reclamation tzn. rozwiązanie musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny i inicjowany bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych, ani na zewnętrznych systemach. Rozwiązanie musi zapewniać mechanizm kompresji danych w trybie in-line. Kompresja musi być integralną częścią systemu macierzowego i nie może być w żaden sposób możliwa do wyłączenia przez administratora macierzy lub serwis producenta. Rozwiązanie musi zapewniać mechanizm deduplikacja danych w trybie in-line. Deduplikacja nie może być w żaden sposób zatrzymywana ani możliwa do wyłączenia przez administratora macierzy. Deduplikacja danych musi być realizowana na bloku o rozmiarze maksimum 4KB. Dla każdego wolumenu macierzy musi zachodzić jednocześnie kompresja i deduplikacja danych. Niedopuszczalne jest stosowanie tych funkcjonalności zamiennie lub rozłącznie. Baza deduplikowanych bloków musi być globalna, tj. musi obejmować bloki danych zapisanych na wszystkich wolumenach i nośnikach w macierzy, zarządzanych przez wszystkie kontrolery macierzy, niezależnie od skali rozwiązania, ilości wolumenów oraz typu danych przechowywanych na wolumenach i pulach nośników. Rozwiązanie musi prezentować aktualny całkowity współczynnik redukcji danych oraz niezależnie uzysk realizowany poprzez thin-provisioning, globalną deduplikację i kompresję.

22	Wbudowane funkcje macierzy	Rozwiązanie musi oferować funkcję tworzenia natychmiastowych kopii wolumenów oraz oferować możliwość utworzenia przynajmniej 40000 kopii wolumenu. Rozwiązanie musi zapewniać hierarchiczne tworzenie kopii (np. kopia z kopii z kopii). W momencie utworzeni kopia nie może zajmować dodatkowej przestrzeni dyskowej dostępnej dla użytkownika. Nie dopuszcza się rozwiązań, które realizują powyższą funkcjonalność na zasadzie „Kopiowania przy zapisie" (Copy-on-write) Rozwiązanie musi oferować możliwość natychmiastowego odtworzenia wolumenu z dowolnej kopii utworzonej z tego wolumenu bądź znajdującej się w dowolnym miejscu hierarchii kopii tego wolumenu. Odtworzony wolumen musi być natychmiast dostępny dla hosta w trybie read/write. Rozwiązanie musi oferować możliwość natychmiastowego odświeżenia dowolnej kopii z dowolnej innej kopii lub wolumenu w ramach jego hierarchii. Odtworzona kopia musi być natychmiast dostępna dla hosta w trybie read/write. Rozwiązanie musi umożliwiać tworzenie grup spójności, które gwarantują spójne kopiowanie, odtwarzanie i odświeżanie grupy wolumenów. Dane zawarte we wszystkich kopiach muszą być objęte globalną - tj. obejmującą wszystkie nośniki w całej macierzy - deduplikacją i kompresją danych. System operacyjny macierzy musi umożliwiać tworzenie spójnych kopii całych baz danych bądź aplikacji bez wykorzystania dodatkowego, zewnętrznego oprogramowania. Musi istnieć możliwość utworzenia wielu kopii naraz bez wykorzystania dodatkowej przestrzeni na macierzy.
23	Replikacja	Rozwiązanie musi posiadać funkcjonalność replikacji synchronicznej umożliwiające utworzenie z obu macierzy klastra active-active (pomiędzy dwiema serwerowniami zlokalizowanymi w osobnych budynkach) oraz zapewniać wszystkie komponenty sprzętowe niezbędne do realizacji funkcjonalności replikacji. Jeżeli takowe komponenty są używane ich właściwości - typu rozmiar fizyczny - muszą

		zostać wliczone w całkowity rozmiar rozwiązania. Replikacja synchroniczna musi być możliwa dla minimum jednego wolumenu (LUNa) oraz jednocześnie dla wielu wolumenów (LUNów), a zmiana ilości replikowanych wolumenów nie może wymagać zmiany konfiguracji sprzętowej macierzy. Replikacja musi być możliwa do realizacji poprzez protokół FC oraz IP. Utworzony w ten sposób klaster udostępnia ten sam wolumen do odczytu/zapisu na obu zaoferowanych macierzach. Zawartość wolumenów klastra musi być identyczna na obu systemach w każdym momencie realizowania klastra. Rozwiązanie replikacji synchronicznej musi bazować na domyślnych sterownikach MPIO systemów operacyjnych bez konieczności dogrywania dodatkowych sterowników.
24	Replikacja kaskadowa	Rozwiązanie musi umożliwiać kaskadową replikacje asynchroniczną – oznacza to iż każdy wolumen replikujący się synchronicznie do drugiej lokalizacji może być replikowany z lokalizacji drugiej do lokalizacji trzeciej w sposób asynchroniczny.
25	Replikacja JurnalLog	Funkcjonalność replikacji bazującej na JournalLog może być dostarczona zarówno jako mechanizm wbudowany jak również dodatkowa aplikacja zewnętrzna ze wszystkimi wymaganymi komponentami sprzętowymi oraz licencyjnymi. Replikacja powinnaumożliwiać: - testowanie operacji Failover - komunikacje poprzez FC oraz Eth - ustawienie niezależnych schematów kopii migawkowych na macierzach biorących udział w replikacji
26	Ochrona wolumenów przed atakiem ransomware	Oferowany system powinien zapewniać ochronę wolumenów przeciw atakom Ransomware. Dane na wolumenach muszą być albo zabezpieczone przed skasowaniem/nadpisaniem przez nieautoryzowaną operację, albo musi być możliwe natychmiastowe odtworzenie danych z kopii migawkowej zabezpieczonej przed usunięciem na okres minimum 1 miesiąca. Ochrona musi zapewniać mechanizmy uodparniające system macierzowy przed:

		- niepowołanym skasowaniem snapshotów nawet przez użytkownika zalogowanego jako administrator macierzy - umożliwiać integrację z replikacją macierzową - zmianą retencji danych - zmianą czasu/serwera czasu – uniezależnienie macierzy oraz snapshotów od serwera czasu - niepowołaną autoryzacją kasowania danych - wspierać zarówno dostęp plikowy jak i blokowy.
27	Dostęp Plikowy	System musi wspierać : CIFS w wersjach 2.0, 2.1, 3.0.2, 3.1.1 oraz NFS v3 lub równoważny
28	Monitoring	W ramach dostawy systemu macierzowego wymagane jest dostarczenie platformy analityczno-raportującej w postaci portalu dostępnego przez przeglądarkę WWW. Platforma powinna zbierać w sposób automatyczny logi z macierzy oraz prezentować je w postaci grafów i raportów, wymagane są następujące funkcjonalności ww. platformy: a. Wyświetlanie używanej przestrzeni wraz ze wskaźnikiem redukcji danych opartych o algorytmy deduplikacji oraz kompresji bez ThinProvisioningu; globalnie dla macierzy oraz lokalnie dla wolumenu b. Portal musi umożliwiać predykcję przyrostu przestrzeni wraz z analizą przyszłej rozbudowy. c. Wyświetlanie historii wydajności poszczególnych zasobów z uwzględnieniem parametrów: latencji, Read&Write IOps, oraz przepustowości; globalnie dla macierzy oraz lokalnie dla wolumenu d. Możliwość tworzenia raportów z pojemności, wydajności, predykcji przyszłej przestrzeni, logów autoryzacji do urządzenia, poziomu oraz czasu wsparcia technicznego. e. Wyświetlanie statusu wykonanych operacji jak Snapshoty, Replikacja synchroniczna f. Wyświetlanie ostrzeżeń o zagrożeniach informacji o logujących się użytkownikach oraz wykonanych komendach na macierzy. g. Wyświetlanie informacji na temat otwartych oraz zamkniętych spraw serwisowych h. Portal musi umożliwiać symulację przyrostu pojemności w zależności od rodzaju aplikacji

		i. Algorytm weryfikacji poprawnej konfiguracji oraz możliwości upgradu oprogramowania macierzowego. j. Umożliwiać automatyczny upgrade macierzy h. Wyświetlanie poboru systemu wraz wskazówkami optymalizacji.
29	Zarządzanie	Rozwiązanie musi udostępniać graficzną konsolę zarządzającą (GUI) poprzez interfejs Web (HTML5), która umożliwia monitorowanie stanu i obciążenia macierzy. Konsola graficzna jest dostępna poprzez przeglądarkę internetową i jest elementem systemu operacyjnego macierzy. Monitorowanie urządzenia musi być dostępne z panelu GUI administratora macierzy i musi obejmować swoim zakresem dane historyczne z okresu przynajmniej 1 roku wstecz. Rozwiązanie musi umożliwiać monitorowanie: - wykorzystania całkowitej pojemności fizycznej, - wykorzystania pojemności logicznej, - globalnego współczynnika redukcji danych, - wartości transferu danych (w MB/s) oraz ilości operacji (IOPS) Rozwiązanie musi być zarządzane poprzez linię komend (CLI) dostępną poprzez protokół SSH. Dostęp do linii komend poprzez SSH musi być możliwy bez podawania hasła tj. przy wykorzystaniu kluczy uwierzytelniających. Rozwiązanie musi udostępniać interfejs REST API oraz SNMP do komunikacji z zewnętrznymi narzędziami monitorującymi. Macierz musi mieć wbudowane procedury pełnej i automatycznej diagnostyki elementów oraz możliwość natychmiastowego raportowania błędów do administratorów oraz do centrum wsparcia technicznego producenta w trybie 24/7/365.
30	Licencja	Rozwiązanie musi być dostarczone z licencjami na wszystkie dostępne dla systemu funkcjonalności oraz dyski dla maksymalnej do uzyskania w oferowanym modelu pojemności RAW.

3.2.8. Przełączniki SAN – 2 szt.

Lp.	Element/cecha/komponent	Wymagania minimalne
1	Ilość portów FC	Min. 8 aktywnych portów z możliwością rozbudowy do 24 poprzez wykupienie dodatkowych licencji i wkładek SFP+ o gradacji min. 8 portów/licencję.
2	Przepustowość portu	Porty uniwersalne o maksymalnej przepustowości 32Gb, z obsługą przepustowości 16 Gb i 8 Gb z automatycznym wyborem przepustowości (auto-scnsing), obsługa trybu fuli-duplex dla wszystkich wspieranych przepustowości.
3	Interfejsy optyczne	Minimum 8 szt. modułów do transmisji światłowodowej z prędkością min. 32 Gb, SFP+ poprzez kabel światłowodowy wielomodowy z interfejsem LC.
4	Inne funkcje i wyposażenie	1. Obsługa trybów pracy portów FC: F_Port, M_Port (Mirror Port), E_Port, D_Port (Diagnostic Port) 2. Obsługa funkcji POD (Ports on Demand) tj. przydziału licencji dla aktywnych portów FC, 1. Aktywne licencje : 3. b) Wcbtools, ; 1. Zoning, 2. Ports on Demand 4. Możliwość zdalnej aktualizacji firrnware'u switcha 5. Możliwość obsługi funkcjonalności: a) FullFabric (z obsługą do min 235 przełączników FC) b) Fabric Vision c) Trunking d) Advanced Performance Monitoring e) Inter Switch Link (ISL) z przepustowością maks. 256 Gbps f) Adaptive Networking g) Access Gateway mode F_Port and NPIV-enabled N_Port Zamawiający oczekuje dostawy przełączników wyposażonych w standardowy zestaw funkcjonalności (licencji) tj. Full Fabric mode, Access Gateway, Advanced Zoning, Fabric

		Services, Adaptive Networking, Advanced Diagnostic Tools. Pozostałe funkcjonalności mogą być dostępne po rozbudowie przełącznika o opcjonalne licencje. 6. Dedykowany interfejs R.1-45 min 101100 Mbis do zarządzania poprzez sieć Ethernet 7. Dedykowany interfejs RJ-45 lub DB9 do zarządzania poprzez interfejs szeregowy 8. Sygnalizacja aktywnych i podłączonych portów na panelu przednim urządzenia 9. Zarządzanie poprzez przeglądarkę WWW z obsługą połączeń szyfrowanych min. 128-bit SSL oraz poprzez usługę SSH
5	Typ obudowy	Wysokość przełącznika 1U z możliwością montażu w szafie rack 19". Obudowa wyposażona w 4 szt. wentylatorów z kierunku przepływu powietrza Non-port to port side airflow.
6	Zasilanie	Minimum jeden zasilacz 150 W AC (100 - 240 V) z gniazdem zasilającym typu IEC 320-C14.

3.2.9. Przełączniki LAN 10\25 GbE – 2 szt.

Lp.	Element/cecha/komponent	Wymagania minimalne
1	Wymagane interfejsy	a. 48 portów 1/10/25GE bezpośrednio w obudowie przełącznika lub na karcie liniowej przełącznika modularnego b. 6 portów definiowanych za pomocą wkładek QSFP, bezpośrednio w obudowie przełącznika lub na karcie liniowej, przy czym każdy z tych portów QSFP posiada możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps Zamawiający wymaga dostarczenia następujących wkładek: a. 16 szt. wkładek 25 Gbps SFP28 b. 2 szt. wkładek 10 Gbps SFP+ c. 2 szt. wkładek 40 Gbps QSFP
2	Pamięć	a. Min. 64 GB pamięci Flash b. Min 24 GB pamięci DRAM
3	Parametry wydajnościowe	a. Prędkość przełączania „wirespeed” dla każdego portu przełącznika

		b. Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3 c. Obsługiwana łączna przepływność (pasmo) min. 3 Tbps d. Obsługiwana łączna przepustowość przełącznika min. 1 miliard pakietów na sekundę (bpps) e. opóźnienie przełączania pakietów nie większe niż 2 µs
4	Funkcjonalności L2	a. Trunking IEEE 802.1Q VLAN; b. Wsparcie dla min. 4000 sieci VLAN; c. Funkcjonalność izolowania portów znajdujących się w tym samym VLAN d. Wsparcie sprzętowe dla minimum 90 tysięcy adresów MAC e. IEEE 802.1w Rapid Spanning Tree (RST) f. IEEE 802.1s Multiple Spanning Tree (MST) g. Wsparcie sprzętowe dla tunelowania QinQ h. Zabezpieczenie przeciwko incydentom w topologii Spanning Tree i. Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach j. Link Aggregation Control Protocol (LACP): IEEE 802.3ad z możliwością zgrupowania minimum 32 interfejsów fizycznych w wiązce k. Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów);
5	Funkcjonalności L3	a. Sprzętowe przełączanie pakietów w warstwie L3 b. Routing w oparciu o trasy statyczne c. Routing w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6. d. Policy Based Routing (PBR) dla IPv4 i IPv6 e. Możliwość uruchomienia sprzętowego load balancera dla protokołów IPv4 i IPv6 ze wsparciem dla tworzenia grup serwerów i adresów VIP, próbkowania serwerów, wyboru ruchu na podstawie protokołu/portu L4 i poprzez filtra ACL f. VRRP v3 g. Statyczny i dynamiczny NAT h. Internet Group Management Protocol (IGMP) Versions 2, 3; i. Wsparcie dla BFDv6 (Bidirectional Forwarding Protocol) j. Wsparcie sprzętowe dla minimum 768 tysięcy prefixów LPM/ wpisów hosta w tablicy routingu IP

		k. Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode I tryb SSM (Source Specific Multicast) l. Wsparcie dla IGMPv3 oraz MSDP m. Wsparcie dla Microsoft NLB n. Wsparcie sprzętowe dla minimum 32,000 tras multicastowych o. Wsparcie dla minimum 1000 instancji VRF wraz z funkcjonalnością importu/eksportu tras (route leaking) p. Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP) q. Minimum 1000 wejściowych oraz 1000 wyjściowych wpisów dla ACL - access control list r.
6	Bezpieczeństwo sieci	a. Wejściowe ACL (standardowe oraz rozszerzone); b. Standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu; c. Standardowe oraz rozszerzone ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP); d. ACL oparte o VLAN-y (VACL); e. ACL oparte o porty (PACL); f. DHCP Snooping g. ARP Inspection h. IP Source Guard i. Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast
7	Szyfrowanie transmisji danych	Przełącznik posiada sprzętowe wsparcie dla szyfrowania portów Ethernet z wykorzystaniem technologii MacSec IEEE 802.1ad na blokach 128 bit oraz 256 bit oraz wykorzystaniem trybu GCM-AES-XPN.
8	Jakość usług w sieci (QoS)	Przełącznik wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci: a. Layer 2 IEEE 802.1p (CoS); b. Klasyfikacja QoS w oparciu o listy (ACL (Access control list) – w warstwach 2, 3, 4; Klasyfikacja ruchu musi odbywać się w zależności, od co najmniej: interfejsu, typu ramki Ethernet, sieci VLAN, priorytetu w warstwie 2 (802.1p), adresów MAC, adresów IP, wartości pola ToS/DSCP w nagłówkach IP, portów TCP i UDP. c. Kolejkowanie na wyjściu w oparciu o CoS 802.1p;

		d. Bezwzględne (strict-priority) kolejkowanie na wyjściu; e. Kolejkowanie WRR (Weighted Round-Robin) na wyjściu lub mechanizm odpowiadający f. Ograniczanie ruchu (policing) do zadanej przepływności na interfejsach wejściowych i wyjściowych g. Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych h. Protokół PFC (Priority Flow Control) IEEE 802.1Qbb i. Urządzenie musi posiadać architekturę pamięci przystosowaną dla obsługi buforów, QoS oraz ruchu typu microburst zapewniając skuteczną obsługę zarówno małych jak i bardzo dużych przepływów danych. Urządzenie musi potrafić monitorować wykorzystanie buforów i sygnalizować przekraczanie zdefiniowanych przez użytkownika progów wielkości przepływu przypadku zaistnienia zjawiska microburst (chwilowe wzrosty ruchu).
9	Zarządzanie	a. Port zarządzający 100/1000 Mbps; b. Port konsoli CLI; c. Zarządzanie In-band; d. SSHv2; e. Authentication, authorization, and accounting (AAA); f. RADIUS; g. TACACS+ h. SNMP v1, v2, v3; i. RMON (przynajmniej grupy Events, Alarms) j. sFlow lub netFlow k. Wsparcie sprzętowe dla telemetrii przepływów z możliwością eksportu z wykorzystaniem protokołu gRPC l. IEEE 802.1ab LLDP m. 802.1x i dynamiczny przydział VLAN do portu n. Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback) o. Role-Based Access Control RBAC; p. Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing) q. Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu. (mirror) r. Network Time Protocol (NTP); s. Precision Time Protocol IEEE 1588 t. Diagnostyka procesu BOOT;

		u. Ping v. Traceroute
10	Rozszerzenia lub gniazda rozszerzeń	Przełącznik posiada możliwość dołączania zewnętrznych, wyniesionych modułów lub przełączników GigabitEthernet oraz 10 GigabitEthernet. Dołączenie modułów lub przełączników nie jest realizowane z wykorzystaniem mechanizmów L2 (Spanning Tree) ani L3 a jedynie w ramach domeny fizycznej bądź stosu urządzeń. Porty modułu wyniesionego są udostępniane do zarządzania i monitorowania z poziomu przełącznika macierzystego.
11	Obudowa	Obudowa o rozmiarach maksymalnie 1RU (rack unit), przeznaczona do montażu w szafie rackowej 19”, w wypadku zastosowania przełącznika modularnego dopuszcza się większy rozmiar urządzenia
12	Zasilacz	Przełącznik musi być wyposażony w 2 zasilacze 230V AC pracujące w konfiguracji redundantnej
13	Chłodzenie	wentylatory w konfiguracji zapewniającej wyrzut ciepłego powietrza od strony portów liniowych
14	Ukompletowanie	Należy dostarczyć wkładki: 25GBASE-SR – 16 szt. 10GBASE-SR – 8 szt Kabel 100GBASE QSFP z medium światłowodowym (tzw. AOC- Active Optical Cable) o długości 2 metrów – 1 szt. Kabel 10GBASE-CU SFP+ o długości 3 m. – 2 szt. Zastosowane wkładki nie mogą ograniczać dostępu do pomocy technicznej producenta – muszą być wspierane przez producenta przełącznika.
15	Serwis	Serwis urządzenia na 36 miesięcy w trybie wymiany niesprawnego urządzenia na nowe na następny dzień roboczy, dostawa urządzenia w trakcie godzin pracy (8x5xNBD)

3.2.10. Przełączniki LAN 1 GbE – 1 szt.

Lp.	Element/cecha/komponent	Wymagania minimalne
1	Wymagane interfejsy	24 porty 10/100/1000BaseT RJ-45 bezpośrednio w obudowie przełącznika lub na karcie liniowej przełącznika modularnego. 4 porty 10G SFP możliwe do obsadzenia wkładkami

		• Gigabit Ethernet 1000Base-SX, • Gigabit Ethernet 1000Base-LX/LH, • 10Gigabit Ethernet 10GBase-SR, • 10Gigabit Ethernet 10GBase-LR, • 10Gigabit Ethernet typu twinax (SFP+ - SFP+) Zamawiający wymaga dostarczenia 2 szt. wkładek 10Gigabit Ethernet 10GBase-SR,
2	Pamięć	Pamięć DRAM – 512 MB Pamięć flash – 256 MB Wielkość bufora pakietów - 1.5 MB
3	Parametry wydajnościowe	Przepustowość przełącznika 128 Gb/s (full duplex), Obsługiwana łączna przepustowość przełącznika min. 40 milionów pakietów na sekundę (Mpps) 256 aktywnych sieci VLAN 15000 adresów MAC 16 statycznych tras IPv4 16 statycznych tras IPv6 64 interfejsów SVI L3 Obsługa MTU-L3 9198B Obsługa ramek Ethernet Jumbo 10240B 1024 grupy IGMP 6 połączeń zagregowanych typu „port channel”

		16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP Ilość wpisów w listach kontroli dostępu Security ACL – 600 ilość wpisów w listach kontroli dostępu QoS ACL – 600
4	Funkcjonalności L2/L3	Routing statyczny dla IPv4 i IPv6, Obsługa IGMPv1/2/3 i MLDv1/2 Snooping IEEE 802.1w Rapid Spanning Tree Per-VLAN Rapid Spanning Tree (PVRST+) IEEE 802.1s Multi-Instance Spanning Tree Obsługa 64 instancji protokołu STP Obsługa protokołu LLDP i LLDP-MED. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC Urządzenie wspiera połączenia link aggregation zgodnie z IEEE 802.3ad Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego Możliwość uruchomienia funkcji serwera DHCP Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.),

5	Bezpieczeństwo sieci	Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level), Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN, Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL, Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X, Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC, Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X, Możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem (multidomain authentication), Możliwość obsługi żądań Change of Authorization (CoA) Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www), Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,

		Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+, Obsługa list kontroli dostępu Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, filtracja na bazie informacji L2 (adresy MAC) jak również na bazie informacji L3 (adresy IP), Funkcja Private VLAN, Przełącznik umożliwia lokalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizm SPAN z możliwością obsługi do 4 sesji monitorujących
6	Bezpieczeństwo oprogramowania i urządzenia	sprawdzanie autentyczności oprogramowania przed uruchomieniem urządzenia, bezpieczna sekwencja uruchamiania, sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.
7	Jakość usług w sieci (QoS)	Implementacja 4 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi, Implementacja algorytmu Shaped Round Robin dla obsługi kolejek, Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),

		Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP, Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z możliwością skonfigurowania minimum 64 różnych ograniczeń, Kontrola sztormów dla ruchu broadcast/multicast/unicast, Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;
8	Zarządzanie	Urządzenie posiada funkcjonalność zarządzania przez 1 adres IP grupą (klastrem) do 8 urządzeń pochodzących z tej samej rodziny przełączników połączonych portami uplinkowymi Obsługa protokołu NTP Obsługa protokołu sFlow dla wszystkich portów fizycznych uplinkowych i downlinkowych dla ruchu w kierunku wejściowym i wyjściowym z możliwością skonfigurowania 2 różnych kolektorów ruchu sFlow, Port konsoli, Dostęp bezprzewodowy Bluetooth do interfejsu zarządzającego urządzenia (telnet, ssh) przez zastosowanie zewnętrznego urządzenia Bluetooth podłączonego do portu USB przełącznika, Plik konfiguracyjny urządzenia możliwy do edycji w

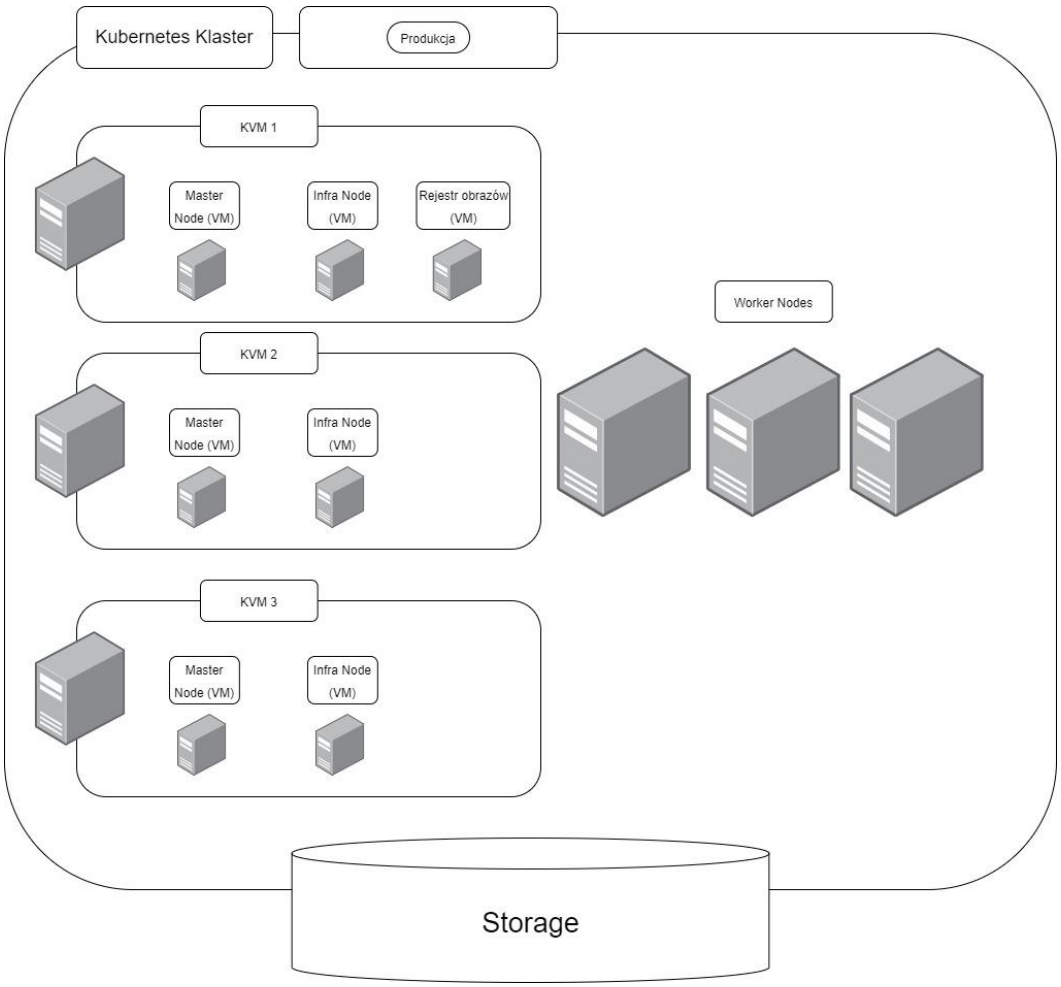
		trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją, Obsługa protokołów SNMPv3, SSHv2, https, syslog, Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu upgradu oprogramowania urządzenia, Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki;
9	Obudowa	Możliwość montażu w szafie rack 19". Wysokość urządzenia 1 RU,
10	Zasilacz	Urządzenie wyposażone jest w wbudowany zasilacz AC230V
11	Serwis	Serwis urządzenia na 36 miesięcy w trybie wymiany niesprawnego urządzenia na nowe na następny dzień roboczy, dostawa urządzenia w trakcie godzin pracy (8x5xNBD)

3.2.11. Platforma zarządzania kontenerami

3.2.11.1. Wstęp

Wykonawca jest zobowiązany do wdrożenia platformy aplikacyjnej Kubernetes przeznaczonej do budowy, uruchomienia i zarządzania aplikacjami systemu SZIRS.
Opisana poniżej platforma aplikacyjna w oparciu o rozwiązanie Kubernetes jest uniwersalnym środowiskiem, na którym mogą być implementowane rozwiązania aplikacyjne różnych producentów w wersji komercyjnej jak i społecznościowej. Dodatkowo dostarczana platforma musi umożliwiać implementację na różnego typu infrastrukturach zaczynając od rozwiązań w modelu on-premise takich jak implementacja platformy bezpośrednio na sprzęcie (ang. Bare metal), na środowisku zwirtualizowanym jak i w modelu chmury obliczeniowej dostarczanej przez jednego lub wielu dostawców takich jak Microsoft, Amazon, IBM, Google, itp.

3.2.11.2. Ogólna architektura aplikacyjnej platformy kontenerowej Kubernetes

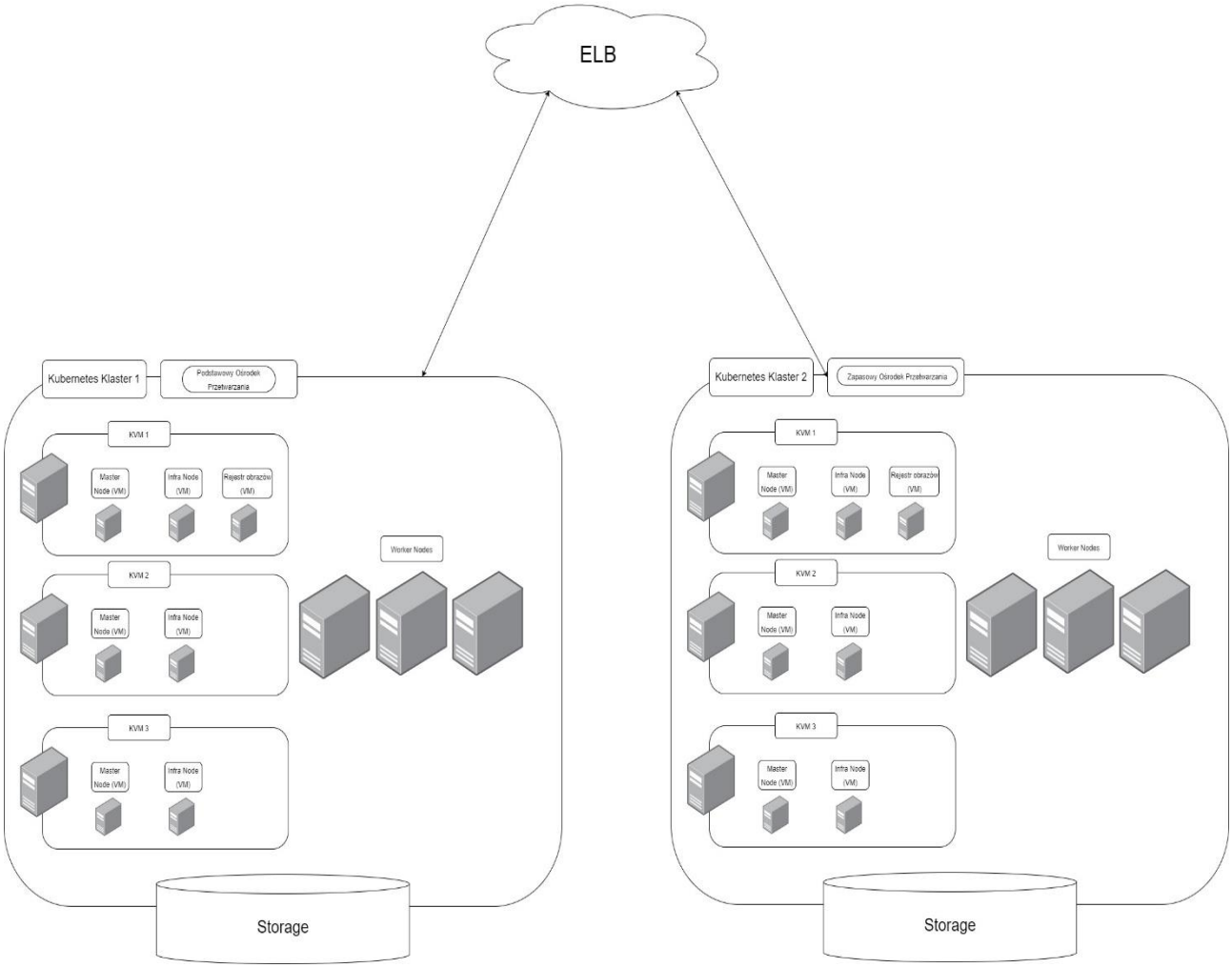


3.2.11.3. Proponowana architektura pojedynczego klastra Kubernetes.

Przedstawiony powyżej rysunek Ogólnej architektury przedstawia schemat implementacji rozwiązania Kubernetes pozwalający na maksymalne wykorzystanie zasobów sprzętowych przeznaczonych dla aplikacji biznesowych poprzez zastosowanie jako Worker Node-y (węzły typu Worker) implementowanych bezpośrednio na sprzęcie. Pozostałe elementy klastra Kubernetes należy zaimplementować jako maszyny wirtualne na niezależnych maszynach fizycznych (Master Node). Takie podejście pozwala na maksymalne wykorzystanie zasobów sprzętowych przeznaczonych dla aplikacji biznesowych oraz pozwala na bezpieczne zarządzanie wszystkimi elementami zarządzającymi i pomocniczymi klastra Kubernetes.

Wirtualizacja zasobów zarządzających i pomocniczych pozwala na optymalizację kosztów środowiska kontenerowego jednocześnie zapewniając elastyczną rozbudowę zarówno części aplikacyjnej jak i komponentów pomocniczych.

3.2.11.4. Architektura aplikacyjnej platformy kontenerowej Kubernetes dla dwóch ośrodków przetwarzania danych w ramach ewentualnej rozbudowy w przyszłości



3.2.11.5. Architektura wysoko-dostępna środowiska Kubernetes

Powyższy rysunek przedstawia schemat implementacji architektury przeznaczonej dla aplikacji pracujących aktywnie w dwóch ośrodkach przetwarzania danych i pozwalających na równoległy dostęp do zasobów w obu ośrodkach.

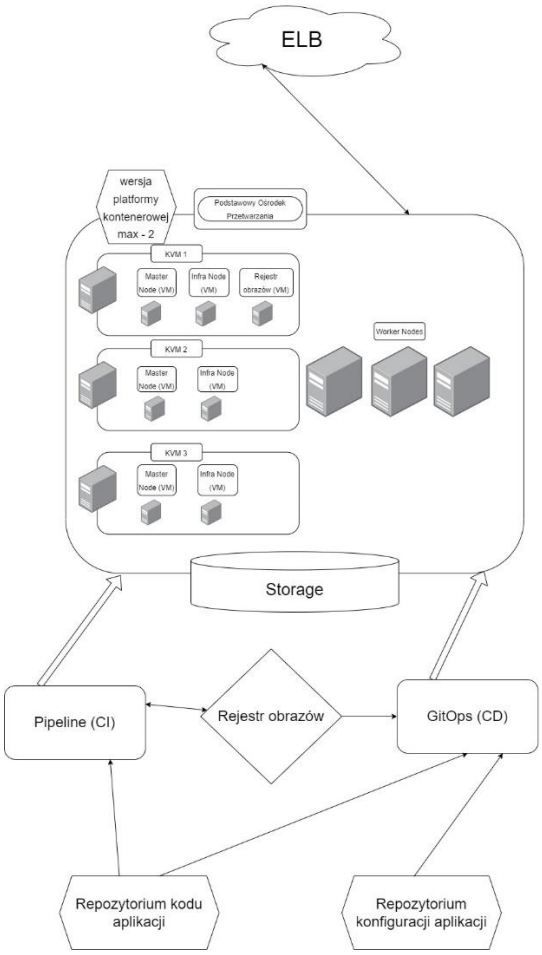
Wdrożona architektura po rozbudowie o drugi ośrodek przetwarzania musi pozwalać na równoległą pracę aplikacji w obu ośrodkach oraz zapewniać użytkownikom dostęp do aplikacji biznesowych w przypadku awarii całego ośrodka.

Replikacja danych pomiędzy ośrodkami musi być realizowana na poziomie aplikacji (np. na poziomie Bazy Danych).

Takie podejście pozwala na uniezależnienie się od komponentów infrastruktury i umożliwia w przyszłości łatwą wymianę komponentów infrastrukturalnych na rozwiązania nowsze i/lub innych producentów bez konieczności modyfikacji architektury rozwiązania jak i kodu aplikacji biznesowych.

Zastosowany mechanizm replikacji będzie zależny od zastosowanego rozwiązania przechowującego dane (np. od rodzaju i typu zastosowanej bazy danych) . Zamawiający wymaga zastosowania relacyjnej bazy danych umożliwiającej wykorzystanie mechanizmów replikacji synchronicznej i asynchronicznej.

3.2.11.6. Architektura rozwiązania CI/CD dla aplikacyjnej platformy kontenerowej Kubernetes



3.2.11.7. Rozwiązanie CI/CD dla platformy Kubernetes

W celu zapewnienia możliwości budowy nowych wersji oprogramowania (upgrade i dodawanie nowych funkcjonalności) oraz dostarczenia wytypowanych wersji aplikacji do wszystkich klastrów Zamawiający wymaga zastosowania mechanizmu automatyzacji CI/CD.
Powyższy diagram przedstawia mechanizm i główne komponenty rozwiązania CI/CD, w których skład wchodzą cztery podstawowe moduły:

- Repozytorium kodu aplikacji i konfiguracji
- Rejestr obrazów

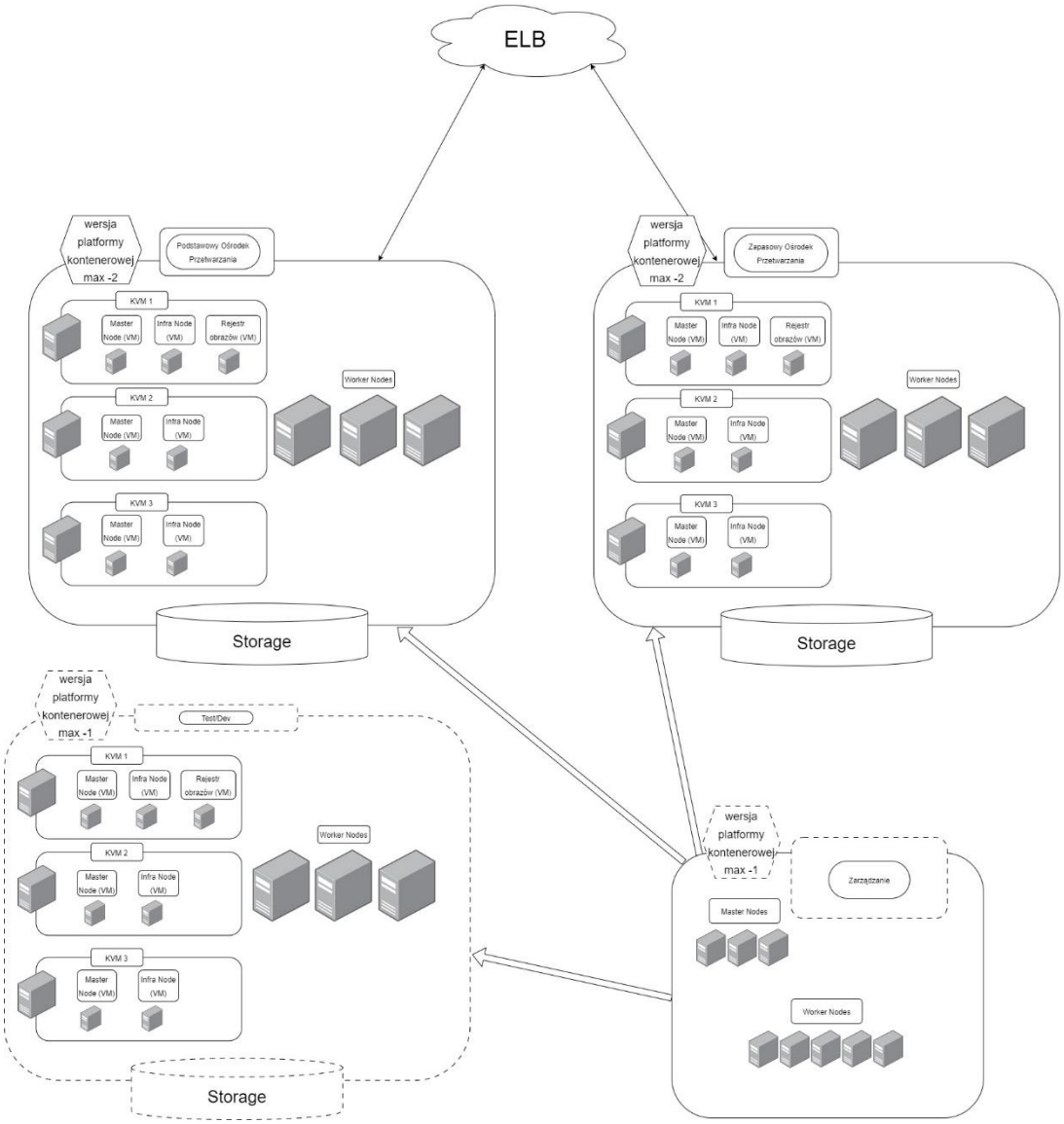
- Komponent Pipeline (CI)
- Komponent GitOps (CD)

Pierwsze dwa moduły muszą zostać zaimplementowane wraz z elementami kontrolnymi klastrów w postaci rozwiązań zwirtualizowanych, natomiast dwa pozostałe to komponenty funkcjonalne klastra Kubernetes, które mogą zostać uruchomione na jednym z klastrów środowiska produkcyjnego, a w przyszłości mogą zostać przesunięte do dedykowanego klastra Kubernetes przeznaczonego na zadania Testowo-Rozwojowe.

Rozwiązanie CI musi zapewnić na niezależne przygotowanie nowych wersji aplikacji biznesowych wraz z możliwym automatycznym testowaniem komponentów i całych modułów aplikacji już na etapie ich budowania. Przy pozytywnym zakończeniu całego procesu wszystkie wymagane komponenty i artefakty są eksportowane do rejestru obrazów i/lub pozostałych rejestrów.

W przypadku podjęcia decyzji o dostarczeniu na środowisko/a produkcyjne nowej wersji aplikacji biznesowej osoba/zespół odpowiedzialne za taki proces ustawiają pożądaną wersję aplikacji biznesowej w repozytorium konfiguracji. Cały proces dostarczenia i uruchomienia wszystkich wymaganych komponentów aplikacji wykonuje moduł GitOps (CD) automatycznie.

3.2.11.8. Docelowa architektura dla aplikacyjnej platformy kontenerowej Kubernetes (rozwiązanie docelowe – po rozbudowie na dwa ośrodki przetwarzania oraz o środowisko Testowo-Rozwojowe na dedykowanym klastrze).



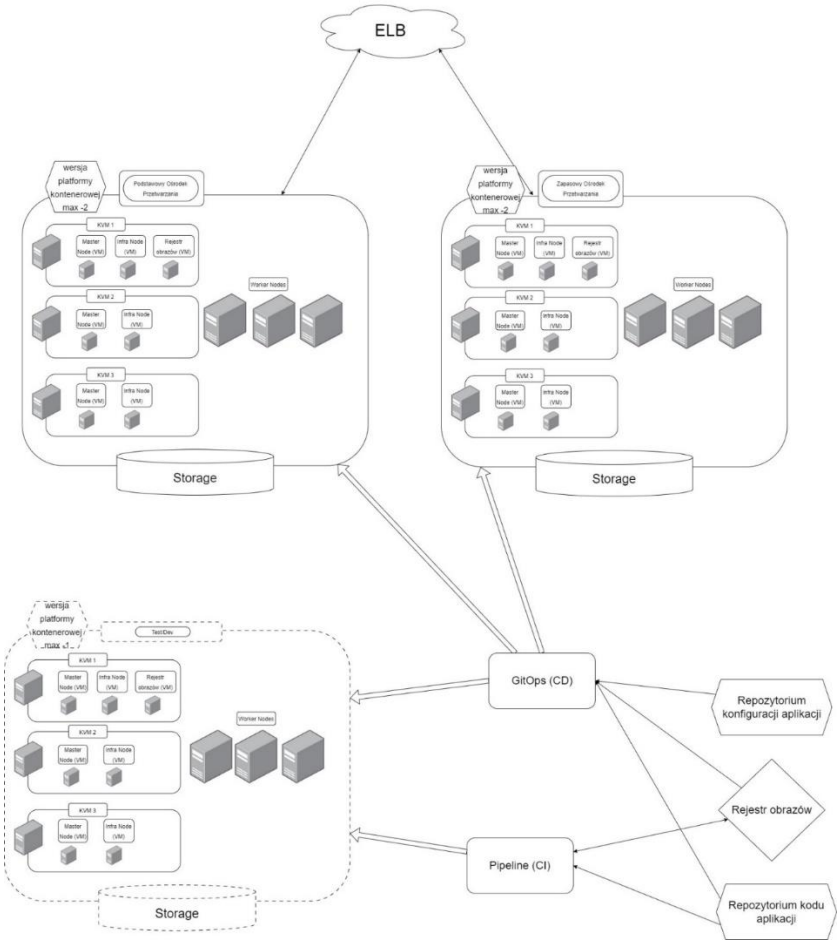
3.2.11.9. Opis docelowa architektury platformy aplikacji kontenerowych Kubernetes (rozwiązanie docelowe – po rozbudowie na dwa ośrodki przetwarzania oraz o środowisko Testowo-Rozwojowe na dedykowanym klastrze)

Punkt ten opisuje wymagania dotyczące ścieżki rozwoju (rozbudowy) platformy aplikacji kontenerowych w przyszłości.

Dobrą praktyką dla poprawnego utrzymania środowiska opartego o rozwiązanie Kubernetes jest posiadanie poza środowiskiem Produkcyjnym niezależnego środowiska Testowo-Rozwojowego.

Architektura przedstawiona na powyższym diagramie jest rozbudowana o dodatkowe środowisko Testowo-Rozwojowe zaimplementowane jako niezależny klaster Kubernetes.

Taka architektura pozwoli w przyszłości na zaimplementowanie elementów Centralnie Zarządzających wszystkimi klastrami jak i umożliwi implementację narzędzia przeznaczonego dla działu bezpieczeństwa pozwalającego na monitorowanie i implementację polityk bezpieczeństwa dla wybranych lub wszystkich posiadanych klastrów Kubernetes.
Dodatkowo taka architektura pozwoli równolegle przeprowadzać proces implementacji nowych wersji aplikacji biznesowych przy pomocy rozwiązań CI/CD jak i umożliwi zaimplementowanie procesu podnoszenia (upgrade-u) platformy Kubernetes z jednoczesnym procesem testów aplikacji biznesowych na nowej wersji platformy.
Docelową architekturę rozwiązania wraz z zaimplementowanym procesem CI/CD przedstawia poniższy diagram.



3.2.11.10. Wymagania funkcjonalne aplikacyjnej platformy kontenerowej Kubernetes

Lp.	Wymagania minimalne
1	W ramach postępowania wymagane jest dostarczenie i uruchomienie aplikacyjnej platformy kontenerowej Kubernetes dla minimum 3 fizycznych serwerów (po osiem procesorów CPU każdy, po dwa na pojedynczy ośrodek przetwarzania).
2	Platforma musi mieć możliwość instalacji na platformach sprzętowych: x86, ARM, IBM Power, zgodnie z dostępną oficjalnie matrycą kompatybilności producenta Platformy

3	Platforma musi mieć możliwość instalacji w chmurze publicznej Amazon Web Service, Microsoft Azure, Google Cloud Engine, IBM Cloud i Alibaba Cloud lub innej
4	Narzędzie do instalacji platformy muszą umożliwiać przeprowadzenie instalacji na wyżej wymienionych platformach w sposób zautomatyzowany tj. narzędzie do instalacji wygeneruje potrzebne do instalacji komponenty infrastruktury takie jak maszyny wirtualne i zainstaluje na nich Platformę
5	Narzędzie do instalacji platformy muszą umożliwiać przeprowadzenie instalacji na wyżej wymienionych platformach w sposób manualny tj. w taki sposób, że administrator może manualnie przygotować wszystkie komponenty infrastruktury potrzebne do instalacji Platformy
6	Narzędzie do instalacji umożliwia instalację platformy na infrastrukturze bez dostępu do sieci internet oraz a infrastrukturze gdzie dostęp do sieci internet jest możliwy tylko przez serwery proxy
7	Platforma umożliwia instalację w konfiguracji wysokiej dostępności bez pojedynczego punktu awarii, gdzie każdy komponent Platformy mający wpływ na jej dostępność będzie uruchomiony w co najmniej dwóch aktywnych instancjach
8	Platforma umożliwia instalację klastra rozciągniętego na więcej niż jeden niezależny ośrodek przetwarzania danych
9	Platforma musi umożliwiać przeprowadzenie aktualizacji wersji oraz instalację poprawek Platformy oraz systemu operacyjnego, na którym jest zainstalowana Platforma w ramach jednolitej i automatycznej procedury aktualizacji
10	W przypadku instalacji Platformy na infrastrukturze bez dostępu do sieci internet istnieje możliwość przeprowadzenia jednolitej i automatycznej procedury aktualizacji Platformy w oparciu o wcześniej pobraną aktualizację zgodnie z dokumentacją producenta Platformy
11	Platforma musi zawierać mechanizm skalowania węzłów klastra w sposób deklaratywny bez konieczności manualnej instalacji i konfiguracji węzłów
12	Platforma musi umożliwiać izolację aplikacji przy użyciu technologii kontenerów w taki sposób, że na jednej instancji systemu operacyjnego równocześnie może być uruchomionych wiele odizolowanych aplikacji mających dostęp do ograniczonych zasobów systemowych takich jak pamięć RAM, moc procesora i system plików
13	Do izolacji kontenerów na poziomie systemu operacyjnego Linux wykorzystywane są mechanizmy SElinux, Cgroups, Namespaces
14	Platforma musi umożliwiać deklaratywne definiowanie limitów zasobów systemowych takich jak pamięć RAM, moc procesora i przepustowość sieci, które będą dostępne dla całej aplikacji jak i dla poszczególnych kontenerów aplikacji

15	Platforma musi umożliwiać deklaratywne definiowanie globalnych limitów zasobów systemowych takich jak pamięć RAM, przestrzeń dyskowa i moc procesora, które są współdzielone przez wiele aplikacji
16	Platforma musi zawierać wbudowany mechanizm umożliwiający automatyczną optymalizację konfiguracji limitów zasobów systemowych przypisanych do kontenerów w oparciu o analizę faktycznej konsumpcji zasobów przez te kontenery
17	Platforma musi umożliwiać separację logiczną poszczególnych aplikacji, projektów (multi tenancy) w taki sposób, że określony tenant może być odseparowany logicznie w warstwie sieciowej, systemu plików, węzłów klastra, dostępu do narzędzi administracyjnych i dla programistów oraz na poziomie systemu operacyjnego
18	Platforma musi zawierać wbudowany rejestr obrazów OCI (Open Container Initiative)
19	Platforma musi pozwalać na uruchamianie aplikacji stanowych, które zapisują i odczytują dane z trwałego nośnika poprzez następujące interfejsy: NFS, Ceph RDB, CephFS, Openstack Cinder, iSCSi, Fibre Channel, Google GCE Volumes, Amazon EBS Volumes, Azure Disk, Azure File, VMWare VMDK
20	Platforma musi pozwalać na wykorzystywanie przez aplikacji stanowe lokalnych zasobów dyskowych znajdujących się na węzłach klastra takich jak lokalne dyski, partycje i urządzenia blokowe
21	Platforma musi umożliwiać instalację sterowników Kubernetes CSI (Container Storage Interface)
22	Platforma musi umożliwiać automatyczny dostęp aplikacjom kontenerowym do wyspecjalizowanych urządzeń i sterowników dostępnych na poszczególnych węzłach klastra takich jak np: GPU poprzez odpowiednie etykietowanie węzłów
23	Platforma musi zawierać mechanizm tuningu węzłów klastra w celu optymalizowania ich wydajności pod kątem wymagań wydajnościowych uruchamianych aplikacji w oparciu o zdefiniowane profile konfiguracji węzłów klastra
24	Platforma musi umożliwiać synchronizację czasu na węzłach klastra z wykorzystaniem protokołu NTP (Network Time Protocol) oraz przy użyciu zainstalowanych na węzłach klastra urządzeń PTP (Precision Time Protocol)
25	Platforma musi zawierać wbudowaną wewnętrzną wirtualną sieć (SDN) umożliwiającą komunikację pomiędzy aplikacjami i usługami uruchomionymi na Platformie oraz dwukierunkową komunikację na zewnątrz
26	Platforma musi umożliwiać konfigurację sieci wewnętrznej w taki sposób, żeby poszczególne aplikacje mogły być od siebie sieciowo odizolowane i jakakolwiek komunikacja pomiędzy aplikacjami była zablokowana
27	Platforma musi umożliwiać w sieci wewnętrznej zastosowanie równocześnie adresacji IPv4 i IPv6

28	Platforma musi umożliwiać mikro segmentację sieci wewnętrznej w taki sposób, że można precyzyjnie określić jakie usługi mogą się komunikować z innymi usługami z dokładnością do portu
29	Platforma musi zawierać wbudowany moduł komunikacyjny (ingress router) umożliwiający komunikację protokołami HTTP, HTTPS, Websocket i TLS with SNI z aplikacjami uruchomionymi na platformie przez systemy uruchomione poza platformą oraz użytkowników aplikacji
30	Platforma musi umożliwiać jednoczesne uruchomienie dwóch wersji aplikacji lub usługi i procentowe rozdzielenie ruchu sieciowego do poszczególnych wersji
31	Moduł komunikacyjny (ingress router) musi pozwalać na terminację SSL, reekrypcję SSL oraz przekazanie połączenia SSL bezpośrednio do kontenera
32	Platforma musi umożliwiać uruchomienie dla aplikacji dedykowanego modułu komunikacyjnego (ingress router), który będzie obsługiwał tylko ruch przychodzący do danej aplikacji
33	Platforma musi umożliwiać komunikację SSL w sieci wewnętrznej pomiędzy wybranymi usługi bez konieczności implementacji logiki komunikacji SSL w poszczególnych usługach
34	Platforma musi umożliwiać szyfrowania komunikacji w sieci wewnętrznej pomiędzy węzłami klastra przy użyciu IPSec lub TLS
35	Platforma musi pozwalać na taką konfigurację aplikacji, żeby cały ruch sieciowy ze wszystkich usług danej aplikacji wychodził poza Platformę tylko z jednego lub kilku dedykowanych dla danej aplikacji adresów IP bez względu na to, na którym węźle klastra dana usługa jest uruchomiona
36	Platforma musi umożliwiać instalację certyfikowanych sterowników sieciowych Kubernetes CNI (Container Network Interface) pochodzących od różnych dostawców
37	Platforma musi pozwalać na podpięcie wielu interfejsów sieciowych do jednego kontenera
38	Platforma musi umożliwiać uruchamianie aplikacji dostarczanych w formie operatorów Kubernetes oraz Helm charts
39	Platforma musi umożliwiać budowanie kontenerów i uruchamianie aplikacji tworzonych w następujących technologiach: Node.js, Ruby, Perl, PHP, Python bez konieczności definiowania pliku Dockerfile
40	Platforma musi umożliwiać budowanie i uruchamianie aplikacji tworzonych w technologii J2EE bez konieczności definiowania pliku Dockerfile
41	Platforma musi umożliwiać budowanie kontenerów i uruchamianie aplikacji tworzonych w technologii Microsoft .NET Core bez konieczności definiowania pliku Dockerfile

42	Platforma musi umożliwiać budowanie kontenerów i uruchamianie dowolnych bibliotek i platform programistycznych zgodnych z wyżej wymienionymi technologiami bez konieczności definiowania pliku Dockerfile
43	Platforma musi zawierać wbudowane mechanizmy umożliwiające automatyzację budowania kontenerów, wdrożenia i uruchomienia aplikacji bezpośrednio z kodu źródłowego aplikacji bez konieczności definiowania plików Dockerfile
44	Platforma musi zawierać gotowe szablony aplikacji, które umożliwiają po parametryzacji zbudowanie i uruchomienie na platformie aplikacji bez konieczności definiowania pliku Dockerfile oraz plików konfiguracyjnych Kubernetes
45	Platforma musi zawierać gotowe narzędzia umożliwiające automatyczne zbudowanie aplikacji razem z zależnościami w formacie obrazu OCI
46	Platforma musi umożliwiać skonteneryzowanie i uruchomienie aplikacji dostarczonych w postaci binarnej bez konieczności kompilacji kodu źródłowego i tworzenia pliku Dockerfile
47	Obrazy kontenerów zbudowane na platformie muszą dawać możliwość uruchomienia zarówno na innych instancjach platformy jak i poza nią w dowolnym środowisku uruchomieniowym zgodnym z OCI
48	Platforma musi zawierać gotowe narzędzia umożliwiające automatyczne zbudowanie obrazu kontenera opisanego plikiem konfiguracyjnym Dockerfile i jego uruchomienie na Platformie
49	Platforma musi zawierać i umożliwiać uruchomienie z gotowych obrazów OCI kontenera serwletów Tomcat lub równoważnego zgodnego ze standardami java servlet
50	Platforma musi zawierać i umożliwiać uruchomienie z gotowych obrazów OCI aplikacji J2SE 1.8, 11 zbudowanych w oparciu o Spring Boot
51	Platforma musi zawierać mechanizm optymalizacji działania aplikacji Java w kontenerach poprzez możliwość kompilacji aplikacji do wersji natywnej uruchamianej bezpośrednio jako proces w kontenerze bez konieczności uruchamiania maszyny wirtualnej Java (JVM) w tym kontenerze
52	Platforma musi zawierać i umożliwiać uruchomienie z gotowych obrazów OCI serwer pojedynczego logowania (SSO) umożliwiający uwierzytelnianie i autoryzację przy użyciu protokołów OpenID Connect i SAML
53	Platforma musi zawierać i umożliwiać uruchomienie z gotowych obrazów OCI baz danych MySQL, MariaDB, PostgreSQL, MongoDB
54	Platforma musi zawierać wbudowane moduły do implementacji i automatyzacji procesu DevSecOps zgodnie z NIST SP 800-204C: https://csrc.nist.gov/publications/detail/sp/800-204c/final w szczególności: Platforma musi zawierać i umożliwiać uruchomienie na platformie serwera CI/CD Tekton,

	Jenkins Platforma musi zawierać i umożliwiać uruchomienie na platformie serwera GitOps ArgoCD Wbudowany rejestr obrazów kontenerów zgodnych z OCI oraz bibliotekę wspieranych przez dostawcę obrazów bazowych OCI Moduł bezpieczeństwa umożliwiający skanowanie obrazów i bibliotek programistycznych pod kątem występowania luk bezpieczeństwa, analizowanie plików konfiguracyjnych Kubernetes pod kątem bezpieczeństwa, monitorowanie działających w kontenerach procesów i ruchu sieciowego w kontenerach Silnik polityk umożliwiający implementację i egzekwowanie polityk bezpieczeństwa w procesie DevSecOps Wbudowany dedykowany moduł do zarządzania i monitorowania komunikacji sieciowej dla aplikacji zbudowanych w architekturze mikro usług (Service Mesh) Moduł do ciągłego monitorowania zgodności konfiguracji klastra z CIS Kubernetes lub równoważnym Moduł do monitoring aplikacji i śledzenia ruchu wewnątrz aplikacji Moduł do agregacji logów aplikacji i platformy Wszystkie wyżej wymienione komponenty muszą być konfigurowane jako kod i zautomatyzowane przy użyciu dedykowanych narzędzi do automatyzacji
55	Platforma musi zawierać katalog aplikacji umożliwiający uruchomienie umieszczonych tam aplikacji bazujących na operatorach Kubernetes, Helm charts oraz innych mechanizmach umożliwiających tworzenie szablonów aplikacji
56	Dostawca platformy dostarcza rejestr certyfikowanych operatorów Kubernetes, które mogą być instalowane na Platformie manualnie przy użyciu narzędzi administracyjnych wchodzących w skład Platformy oraz automatycznie przy użyciu dedykowanych narzędzi do automatyzacji
57	Platforma musi dawać dostęp do publicznego rejestru obrazów, z którego można pobrać stale aktualizowane i certyfikowane przez dostawcę Platformy wyżej wymienione obrazy OCI
58	Platforma musi zawierać i umożliwiać uruchomienie centralnego serwera agregacji logów aplikacji i Platformy opartego na technologii ElasticSearch, Kibana i Fluentd lub równoważnych który umożliwia długotrwałe przechowywanie logów na trwałych nośnikach danych
59	Platforma musi posiadać wbudowany mechanizm umożliwiający przesyłanie logów do zewnętrznych systemów agregacji i analizy logów takich jak ElasticSearch, Fluentd, Syslog, Kafka, Loki, AWS Cloudwatch
60	Platforma musi zawierać i umożliwiać uruchomienie centralnego serwera agregacji metryk aplikacji działających na Platformie oraz samej Platformy opartego na technologii

	Prometheus lub równoważnej, który umożliwia długotrwałe przechowywanie metryk na trwałych nośnikach danych
61	Platforma powinna umożliwiać zbieranie i przechowywanie metryk oraz logów aplikacji przez określony czas
62	W przypadku uruchamiania aplikacji z obrazów OCI muszą one pozwalać na uruchomienia jako użytkownik systemowy bez pełnych praw administracyjnych
63	Platform musi domyślnie uniemożliwić uruchomienie kontenerów na prawach użytkownika root
64	Platforma musi pozwalać na zautomatyzowane przenoszenie aplikacji pomiędzy różnymi instancjami platformy, które mogą być uruchomione na różnych infrastrukturach (serwery fizyczne, wirtualne, chmura prywatna, publiczna)
65	Platforma musi umożliwiać uruchomienie nowej wersji aplikacji przy zachowaniu pełnej dostępności aplikacji i bez konieczności jej zatrzymania lub ograniczenia dostępności (rolling upgrade)
66	Platforma musi umożliwiać automatyczne cofnięcie wdrożenia aplikacji (deployment) do jednej z poprzednich wersji
67	W przypadku klastrowania aplikacji platforma musi zapewniać mechanizm rozłożenia ruchu pomiędzy instancjami aplikacji (load balancing)
68	Platforma musi umożliwiać podłączenie zewnętrznych komponentów do rozkładania ruchu pomiędzy instancjami aplikacji (zewnętrzny load balancer)
69	Platforma musi umożliwiać uruchamiania wielu aplikacji równocześnie na współdzielonych zasobach sprzętowych
70	Platforma musi zawierać wbudowany mechanizm skalowania, który pozwala określić deklaratywnie, ile instancji danej aplikacji ma być uruchomionych jednocześnie i pozwala na skalowanie ilości uruchomionych jednocześnie instancji aplikacji
71	Platforma musi zawierać wbudowany mechanizm do wdrażania aplikacji w którym skalowanie aplikacji odbywa się dynamicznie w sposób zautomatyzowany bazując na ruchu generowanym do danej aplikacji lub wydajności instancji aplikacji
72	Platforma musi zawierać wbudowany mechanizm obsługi zdarzeń umożliwiający automatyczne skalowanie aplikacji w odpowiedzi na pojawiające się zdarzenia, których źródłem mogą być systemy typu messaging np: Kafka lub HTTP
73	Platforma musi zawierać wbudowane mechanizmy automatycznego skalowania aplikacji (uruchamiania lub wyłączania kolejnych instancji aplikacji) w oparciu o metryki zużycia zasobów systemowych przez aplikację
74	Platforma musi zawierać wbudowaną konsolę administracyjną umożliwiającą wykonywanie zadań administracyjnych przez przeglądarkę internetową

75	Platforma musi zawierać wbudowane narzędzia umożliwiające administrację i konfigurację platformy z poziomu linii poleceń działające na Microsoft Windows, Red Hat Enterprise Linux, MacOSX
76	Platforma musi zawierać wbudowany webowy terminal znakowy, który umożliwia dostęp do narzędzia do administracji i konfiguracji platformy z poziomu linii poleceń poprzez przeglądarkę internetową
77	Platforma musi zawierać wbudowany interfejs programistyczny API dostępny przez protokół REST umożliwiający administrację platformą przy użyciu narzędzi zewnętrznych
78	Platforma musi zawierać wbudowane mechanizmy uwierzytelniania i autoryzacji użytkowników oparte na OAuth 2.0, oraz umożliwia konfigurację dostępu opartego na rolach dla różnych grup użytkowników w tym administratorów i programistów
79	Platforma musi umożliwiać definiowanie różnych projektów dla poszczególnych aplikacji i przypisywania uprawnień do nich dla określonych grup użytkowników
80	Platforma musi pozwalać na integrację z zewnętrznymi bazami użytkowników w tym Microsoft Active Directory lub LDAP oraz serwerami autoryzacji zgodnymi z OAuth 2.0
81	Platforma musi zawierać wbudowany mechanizm umożliwiający administratorom określenie uprawnień dla uruchamianych na platformie kontenerów takich jak uprawnienia użytkownika, dostępu do zasobów sprzętowych oraz profile seccomp
82	Platforma musi umożliwiać przechowywanie konfiguracji klastra i aplikacji Kubernetes na trwałych nośnikach danych w formie zaszyfrowanej
83	Platforma musi zawierać mechanizm konfiguracji systemu operacyjnego z poziomu Platformy bez konieczności manualnej konfiguracji bezpośrednio na systemie operacyjnym
84	Platforma musi zawierać elastyczny silnik polityk, który umożliwia definiowanie i egzekwowanie polityk konfiguracji Platformy i aplikacji wdrożonych na Platformie
85	Platforma musi zawierać wbudowany mechanizm proaktywnego wykrywania, priorytetowania i rozwiązywania problemów wydajnościowych, stabilności i bezpieczeństwa Platformy
86	Platforma musi zawierać wbudowany dedykowany moduł do zarządzania i monitorowania komunikacji sieciowej dla aplikacji zbudowanych w architekturze mikro usług
87	Moduł zarządzania komunikacją sieciową umożliwia zarządzania ruchem wchodzącym i wychodzącym, uwierzytelnianie, autoryzację i szyfrowanie ruchu przez mTLS, możliwość filtrowania ruchu i zarządzania nim w oparciu o zdefiniowane przez administratora reguły
88	Moduł zarządzania komunikacją sieciową musi posiadać wbudowaną konsolę webową umożliwiającą konfigurację i wizualizację komunikacji wewnątrz Service Mesh
89	Moduł zarządzania komunikacją sieciową umożliwia uruchomienie na jednym klastrze wielu niezależnych instancji sieci wraz z oddzielnymi konsolami do zarządzania dla każdej instancji

90	Platforma musi zawierać wbudowany mechanizm śledzenia komunikacji pomiędzy usługami uruchomionymi na Platformie zgodny z OpenTracing API
91	Platforma musi zawierać zintegrowane środowisko programistyczne (IDE), które umożliwia rozwijanie kodu aplikacji, jego kompilację i uruchomienie na platformie bez konieczności wcześniejszej jej konteneryzacji
92	Platforma musi posiadać moduł umożliwiający balansowanie obciążenia poszczególnych węzłów klastra w celu optymalizacji konsumpcji zasobów
93	Platforma musi posiadać narzędzie umożliwiające migrację aplikacji (konfiguracji i danych) pomiędzy różnymi klastrami
94	Wszystkie oferowane komponenty Platformy są oferowane w ramach jednolitego rozwiązania oraz są objęte wsparciem producenta i nie będą dodatkowo instalowane przez dostawcę w ramach wdrożenia będącego przedmiotem tego postępowania
95	Wszystkie platformy kontenerowe traktowane są jako środowiska produkcyjne.

3.2.11.11. Wymagania funkcjonalne rejestru obrazów kontenerów:

Lp.	Wymagania minimalne
1	Rejestr obrazów musi mieć możliwość zainstalowania na klastrze Kubernetes w formie skonteneryzowanej
2	Rejestr obrazów musi mieć możliwość zainstalowania na systemie operacyjnym Linux na maszynach wirtualnych lub serwerach fizycznych
3	Rejestr obrazów musi umożliwiać skanowanie zawartości obrazów OCI pod kątem występowania luk bezpieczeństwa
4	Rejestr obrazów musi umożliwiać ciągłe automatyczne skanowanie obrazów w określonych interwałach czasowych w celu ciągłego wykrywania luk bezpieczeństwa
5	Rejestr obrazów musi umożliwiać prezentację wyników skanowania obrazów OCI bezpośrednio w interfejsie użytkownika klastra Kubernetes
6	Rejestr obrazów musi umożliwiać automatyczne wysyłanie powiadomień w przypadku wykrycie nowej podatności o określonym poziomie (severity) w obrazie, przesłania obrazu do repozytorium lub uruchomienia procedury budowania obrazu
7	Rejestr obrazów musi pozwalać na replikację repozytoriów pomiędzy różnymi instancjami Rejestru rozproszonymi geograficznie
8	Rejestr obrazów musi pozwalać na przechowywanie obrazów na różnych typach przestrzeni dyskowej zarówno lokalnych jak i w chmurach publicznych
9	Rejestr obrazów musi zawierać log audytowy, który umożliwia śledzenie zdarzeń i akcji wywołanych zarówno przez API jaki i interfejs użytkownika

10	Rejestr obrazów musi umożliwiać uruchomienie w konfiguracji wysokiej dostępności bez pojedynczego punktu awarii
11	Rejestr obrazów musi posiadać wbudowany mechanizm uwierzytelniania, który umożliwia uwierzytelnianie użytkowników LDAP oraz przy użyciu protokołów OAuth 2.0 i OpenID Connect.
12	Rejestr obrazów musi pozwalać na przypisanie ról i uprawnień użytkownikom w rozróżnieniem na administratorów Platformy oraz administratorów i użytkowników poszczególnych repozytoriów
13	Rejestr obrazów musi umożliwiać monitorowanie i dostęp do metryk poprzez bazę metryk Prometheus
14	Platforma musi pozwalać na przesyłanie powiadomień o wystąpieniu różnych zdarzeń na platformie oraz w poszczególnych repozytoriach przez Email, Slack oraz Webhook
15	Platforma musi pozwalać na utworzenie kont serwisowych, którym mogą być przypisane różne uprawniania na poziomie Platformy oraz poszczególnych repozytoriów w celu używania przez zewnętrzne aplikacje
16	Rejestr musi umożliwiać jednoczesne przechowywanie obrazów dla różnych typów architektur sprzętowych takich jak x86, IBM Power LE oraz Z System, ARM, Windows

3.2.11.12. Wymagania funkcjonalne modułu bezpieczeństwa kontenerów:

Lp.	Wymagania minimalne
1	Moduł musi mieć możliwość zainstalowania na klastrze Kubernetes w formie skonteneryzowanej i monitorować wiele klastrów zdalnych przy użyciu agentów zainstalowanych lokalnie na tych klastrach
2	Moduł musi udostępniać interfejs użytkownika przez przeglądarkę internetową oraz interfejs programistyczny API
3	Moduł musi umożliwiać śledzenie i wizualizację ruchu sieciowego wewnątrz klastra oraz połączeń na zewnątrz klastra z możliwością filtrowania ruchu do poziomu projektów (namespaces), wdrożeń (deployments) i poszczególnych podów
4	Moduł musi umożliwiać śledzenie procesów uruchomionych w kontenerach i wykrywanie aktywności niezgodnych ze zdefiniowanymi politykami bezpieczeństwa
5	Moduł musi umożliwiać ciągłe skanowanie obrazów w celu wykrycia znanych podatności w bibliotekach systemowych oraz aplikacyjnych uruchamiane automatycznie w określonych interwałach czasowych
6	Moduł musi umożliwiać egzekwowanie zgodności z politykami bezpieczeństwa na każdym etapie życie aplikacji: podczas budowania obrazów kontenerów, podczas wdrażania aplikacji na klastrze i w trakcie działania aplikacji

7	Moduł musi pozwalać na weryfikację zgodności ze standardami i regulacjami takimi jak CIS Benchmarks, Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA) oraz NIST SP 800-190
8	Moduł musi udostępniać raporty zgodności z wyżej wymienionymi standardami i regulacjami oraz umożliwia eksport tych raportów do oddzielnych plików w celu udostępnienia audytorom
9	Moduł musi umożliwiać filtrowanie informacji o zgodności z poszczególnymi standardami i regulacjami na poziomie klastra, węzłów klastra lub projektów (namespaces)
10	Moduł musi umożliwiać automatyczne generowanie polityk sieciowych na podstawie śledzenia ruchu i polityk bezpieczeństwa
11	Moduł musi umożliwiać symulację polityk sieciowych przed ich wdrożeniem w celu analizy ich wpływu na działające aplikacje
12	Moduł musi pozwalać na priorytetyzację ryzyka działania poszczególnych aplikacji na platformie
13	Moduł musi dostarczać gotowe polityki bezpieczeństwa w celu automatycznego wykrywania niezgodności w konfiguracji sieciowej, eskalacji uprawnień w kontenerach, wykrywania procesów uruchamianych jako root i podobnych
14	Moduł musi umożliwiać analizę uprawnień Kubernetes role-based access control (RBAC) przypisanych do użytkowników i kont serwisowych (service accounts)
15	Moduł musi umożliwiać śledzenie zdarzeń w klastrze zapisywanych w Kubernetes audit log w celu wykrywania niezgodności z politykami bezpieczeństwa
16	Moduł musi dostarczać gotowe polityki bezpieczeństwa w celu automatycznego wykrywania oprogramowania crypto mining, eskalacji uprawnień i znanych podatności
17	Moduł musi udostępniać API oraz umożliwiać integrację z zewnętrznymi systemami CI/CD i DevOps, skanerami obrazów, rejestrami obrazów, systemami SIEM i systemami do powiadamiania
18	Moduł musi posiadać mechanizmy do zablokowanie uruchomienia kontenera z obrazu, którego zawartość jest nieznana lub zawiera lukę bezpieczeństwa
19	Moduł musi obsługiwać wszystkie platformy kontenerowe w środowisku Zamawiającego

3.2.11.13. Wymagania funkcjonalne modułu zarządzania środowiskiem hybrydowym (wiele klastrów na wielu infrastrukturach):

Lp.	Wymagania minimalne
1	Moduł musi mieć możliwość zainstalowania na klastrze Kubernetes w formie skonteneryzowanej

2	Moduł musi udostępniać interfejs użytkownika przez przeglądarkę internetową oraz interfejs programistyczny API
3	Moduł musi umożliwiać instalację nowych klastrów Kubernetes oraz zarządzanie istniejącymi klastrami Kubernetes zarówno w infrastrukturze zamawiającego jak i w chmurze publicznej
4	Moduł musi umożliwiać instalację nowych klastrów Kubernetes na platformie AWS, Microsoft Azure, Google Cloud Platform, Microsoft Azure Government, serwery fizycznie, Red Hat OpenStack Platform, VMware vSphere
5	Moduł musi pozwalać na skalowanie węzłów na zarządzanych klastrach
6	Moduł musi pozwalać na definiowanie uprawnień do zarządzania oddzielnie różnymi klastrami i grupami klastrów
7	Moduł musi umożliwiać zbieranie, długoterminowe przechowywanie, retencję i wizualizację metryk wydajności działania zarządzanych klastrów
8	Moduł musi umożliwiać definiowanie własnych metryk i ich wizualizację na Platformie oraz na definiowanie własnych wykresów na Platformie
9	Moduł musi umożliwiać wyszukiwanie obiektów Kubernetes wchodzących w skład danego klastra lub aplikacji
10	Moduł musi zawierać mechanizm tworzenia alertów i wysyłania powiadomień w przypadku wygenerowania oznaczonych alertów
11	Moduł musi zawierać gotowe polityki do konfiguracji zarządzanych klastrów oraz umożliwiające automatyczną instalację dodatkowych komponentów na zarządzanych klastrach przy użyciu operatorów Kubernetes lub Helm charts
12	Moduł musi umożliwiać centralne wdrażanie poprawek dla wykrytych niezgodności z politykami i standardami na zarządzanych klastrach
13	Moduł musi umożliwiać monitorowanie prawidłowego działanie aplikacji zainstalowanych na zarządzanych klastrach oraz wgląd w szczegóły konfiguracji aplikacji
14	Moduł musi pozwalać na automatyczne wdrażanie aplikacji na zarządzanych klastrach zgodnie ze zdefiniowanymi regułami przyporządkowania aplikacji do klastrów
15	Moduł musi pozwalać na automatyczne wdrażanie aplikacji Helm na zarządzanych klastrach zgodnie ze zdefiniowanymi regułami przyporządkowania aplikacji do klastrów
16	Moduł musi udostępniać graficzne narzędzie dostępne przez przeglądarkę internetową umożliwiające konfigurację procedury wdrażania aplikacji na zarządzanych klastrach umożliwiające wybór źródła zawierającego konfigurację aplikacji oraz reguł wyboru klastrów na które aplikacja ma być wdrożona
17	Moduł musi umożliwiać wdrażanie aplikacji na zarządzanych klastrach z wykorzystaniem zewnętrznego narzędzia GitOps np: ArgoCD lub równoważnego

18	Moduł musi pozwalać na wykonanie kopii zapasowej konfiguracji klastra i jego odzyskanie na innym klastrze
19	Moduł musi obsługiwać wszystkie platformy kontenerowe w środowisku Zamawiającego

3.2.11.14. Wymagania funkcjonalne modułu integracji platformy kontenerowej z rozwiązaniami obsługi zasobów dyskowych:

Lp.	Wymagania minimalne
1	Moduł musi mieć możliwość tworzenia wolumenów Kubernetes (Persistent Volume) z trybem dostępu RWO i RWX
2	Moduł musi umożliwiać tworzenia wolumenów Kubernetes typu blokowego i plikowego
3	Moduł musi umożliwiać tworzenie woluminów obiektowych (Object Bucket)
4	Utworzone wolumeny obiektowe muszą być obsługiwane przez interfejs S3
5	Wolumeny obiektowe muszą pozwalać na replikowanie do innych obiektowych systemów pamięci masowych zarówno lokalnych jak i w chmurze publicznej
6	Moduł musi umożliwiać zarządzanie procesem dostarczanie danych rozwiązania dyskowego zarządzanego programowo dla całej platformy kontenerowej

3.2.11.15. Wymagania funkcjonalne rozwiązania dyskowego zarządzanego programowo:

Lp.	Wymagania minimalne
1	Rozwiązanie musi posiadać możliwość serwowania danych za pomocą interfejsów blokowych, plikowych i obiektowych.
2	Rozwiązanie musi działać w formie klastera i gwarantować wydajność, niezawodność i skalowalność.
3	Utworzone wolumeny obiektowe muszą być obsługiwane przez interfejs S3
4	Rozwiązanie musi umożliwiać asynchroniczną replikację danych pomiędzy różnymi klastrami w tym Kubernetes.
5	Musi zawierać mechanizm umożliwiający kontrolę i zarządzanie pojemnością danych w rozwiązaniu
6	Rozwiązanie musi zapewniać niezawodność przechowywanych danych poprzez posiadanie dwóch lub więcej replik danych oraz erasure coding
7	Odporność na awarie i minimalizację prac wymaganych przy utrzymaniu rozwiązania
8	Rozwiązanie musi pozwalać na elastyczną zmianę polityk ochrony danych w trakcie pracy

9	Rozwiązanie musi umożliwiać zbudowanie współdzielonej przestrzeni dyskowej w oparciu o dyski wewnętrzne serwerów fizycznych. Rozwiązanie powinno wspierać następujące konfiguracje serwerów: hybrydowa w oparciu o dyski SSD i HDD oraz all-flash w oparciu o dyski SSD (SAS/SATA/NVMe).
10	Klaster, na którym zostanie zainstalowane Rozwiązanie, musi umożliwiać utworzenie przestrzeni dyskowej złożonej z co najmniej 16 hostów i rozbudowę każdego z hostów do co najmniej 30 dysków
11	Rozwiązanie musi umożliwiać konfigurację serwerów all-NVMe.
12	Rozwiązanie musi umożliwiać zmniejszenie lub zwiększenie przestrzeni dyskowej poprzez: usunięcie, lub dodanie pojedynczego dysku, dwóch i więcej dysków, usunięcie lub dodanie serwera fizycznego w sposób niewymagający przestoju i przerwy w działaniu.
13	Rozwiązanie musi zapewniać możliwość obsługiwania woluminów blokowych do rozmiaru co najmniej 40TB.
14	Rozwiązanie musi zapewniać funkcjonalność konfigurowalnych mechanizmów zabezpieczania danych na wypadek awarii sprzętowej pojedynczego dysku, węzła, szafy Rack oraz całego centrum przetwarzania danych.
15	Lista wspieranych i certyfikowanych konfiguracji serwerów kompatybilnych z rozwiązaniem musi być zamieszczona na oficjalnej stronie producenta tego Rozwiązania. Wymagane jest wsparcie dla min. trzech niezależnych producentów sprzętu serwerowego dostępnego na terenie Unii Europejskiej.
16	Rozwiązanie musi działać w środowiskach bez dostępu do sieci Internet
17	Rozwiązanie musi zapewniać możliwość zarządzania użytkownikami i rolami użytkowników (RBAC)
18	Rozwiązanie musi umożliwiać udostępnianie przestrzeni dyskowej również dla fizycznych serwerów, w oparciu o technologię iSCSI, a także umożliwiać zarządzanie dostępnością, pojemnością i wydajnością bez konieczności ograniczania dostępu do danych.
19	Rozwiązanie musi zawierać interfejs API umożliwiający automatyzowanie wdrażania lub modyfikacji konfiguracji Systemu.
20	Rozwiązanie musi być wspierane jako backup target co najmniej dla 2 producentów systemu backup: CommVault, IBM Spectrum Protect Plus, IBM Spectrum Protect server, NetApp AltaVault, Rubrik Cloud Data Management (CDM), Trilio, Veeam (object storage), Veritas NetBackup for Symantec OpenStorage (OST) cloud backup
21	Rozwiązanie musi umożliwiać tworzenie woluminów Kubernetes (Persistent Volume) z trybem dostępu RWO i RWX
22	Rozwiązanie musi umożliwiać tworzenia wolumniów Kubernetes typu blokowego i plikowego
23	Rozwiązanie musi zawierać wbudowany mechanizm kompresji danych

24	Rozwiązanie musi umożliwiać klonowanie i tworzenie migawek (snapshot) woluminów danych
25	Rozwiązanie musi umożliwiać zdalną replikację danych typu on-line (bez przerywania prezentacji zasobów dyskowych) do rozwiązania tej samej rodziny w trybie asynchronicznym.
26	Rozwiązanie musi zapewniać szyfrowanie danych na poziomie całego klastra
27	Rozwiązanie musi umożliwiać uruchomienie warstwy danych w konfiguracji HA z 3 replikami danych
28	Rozwiązanie musi zapewniać mechanizm bezpiecznego, bezprzerwowego i automatycznego uaktualniania rozwiązania wliczając w to zarówno poprawki bezpieczeństwa, jak i zmianę wersji oprogramowania
29	Rozwiązanie musi posiadać narzędzia kryptograficzne
30	System operacyjny rozwiązania musi posiadać udokumentowany certyfikat bezpieczeństwa zgodny ze standardem ISO/IEC 15408 lub równoważny
31	Rozwiązanie musi pozwalać na obsługę 256TB przestrzeni fizycznej z jej dowolnym podziałem na przestrzeń blokową, plikową lub obiektową. Jeśli oferowane rozwiązanie wymaga licencji/subskrypcji na przestrzeń użytkową należy dostarczyć 0.66%x256TB dla każdego z wymienionych typów wymaganej przestrzeni użytkowej.

3.2.12. System backupu

3.2.12.1. Wstęp

Pojęcie system wskazuje na rozwiązanie zabezpieczające dane stanowiące jedno, spójne rozwiązanie, zarządzane z poziomu jednej konsoli. Nie dopuszcza się rozwiązań pochodzących od różnych producentów, a co za tym idzie nie całkowicie niezintegrowanych pomiędzy sobą wymagających wykorzystywania różnych konsol dla zarządzania czy konfiguracji.
Zamawiający rozumie archiwizację danych, jako proces przenoszenia zasobów plikowych i pocztowych do archiwum (repozytorium dyskowe) po skopiowaniu tych zasobów system musi tworzyć skróty oraz kasować zarchiwizowane dane w pełni automatycznie. Obie funkcjonalności: kasowanie danych i tworzenie skrótów musi być dostępne co najmniej dla archiwizowanych danych plikowych z systemów Windows i Linux, oraz maili z systemów Exchange Onpremis i Exchange Online.
Jeśli przy danym punkcie wymogu występuje informacja „jako opcja” oznacza to, iż zaproponowany system posiada daną funkcjonalność, a jej uruchomienie może wymagać zakupu dodatkowych licencji – Zamawiający nie oczekuje oferty na nią a jedynie chce mieć możliwość w przyszłości rozbudowy o tę funkcjonalność.

W celu weryfikacji funkcjonalności oferowanych przez proponowany system, Zamawiający zastrzega sobie możliwość wezwania do przeprowadzenia wybranych testów funkcjonalnych potwierdzających zadeklarowane funkcjonalności w ciągu 5 dni od daty wezwania. W razie odmowy przeprowadzenia testów lub ich wynik negatywny - pozwala Zamawiającemu odrzucić proponowaną ofertę bez podania przyczyny.

3.2.12.2. Wymogi podstawowe oprogramowania backupowego

1. Rozwiązanie musi reprezentować architekturę trójwarstwową (serwer zarządzający, serwer medialny oraz klient), taka architektura pozwoli na elastyczną skalowalność rozwiązania bez względu na dynamikę przyrostu danych.
2. Oprogramowanie nie może preferować platformy sprzętowej, nie może być profilowane pod konkretnego dostawcę sprzętu serwerowego oraz pamięci masowych. Niedopuszczalne jest aby funkcjonalności związane z zabezpieczaniem danych były w jakikolwiek sposób związane czy zależne od konkretnego typu czy producenta urządzenia.
3. Jeśli system korzysta z bazy danych to wszelkie potrzebne licencje muszą być dostarczone i stanowić całość oferty, z tym iż licencje dla silnika bazodanowego muszą pozwalać na zainstalowanie go: na serwerze fizyczny (minimum 2xCPU po 16 core), klastrze active-passive czy serwerze wirtualnym w środowisku minimum Vmware i Hyper-V.
4. Licencje muszą pozwalać na stworzenie dla serwera zarządzającego rozwiązania wysokodostępnego z częstotliwością replikacji bazy katalogowej nie dłuższym niż 15 minut (RPO nie większe niż 15 min dla uruchomienia zapasowego serwera zarządzającego). Jeśli do stworzenia takowego rozwiązania potrzebne są licencje replikacyjne, klastrowe, współdzielona przestrzeń dyskowa to muszą zostać zaoferowane. Licencje muszą pozwalać na skonfigurowanie serwerów zarządzających oraz ich replikację dla co najmniej trzech lokalizacji, gdzie pierwsza jest lokalizacja produkcyjną, druga i trzecia są typu standby dla serwera zarządzającego.
5. Jako opcja musi istnieć możliwość zainstalowania serwera zarządzającego na systemie operacyjnym Linux z zachowaniem możliwości replikacji bazy katalogowej i tworzeniem serwerów typu standby.
6. Proces przełączenia serwera zarządzającego musi umożliwiać:
   - Przełączenie automatyczne inicjalizowane przez administratora
   - Przełączenie automatyczne (bezobsługowe) w przypadku wykrycia awarii (w przypadku awarii serwera zarządzającego system automatycznie wykrywa awarie i przełącza działanie systemu na serwer zapasowy – standby, bez jakiejkolwiek interwencji administratora)
7. Przełączenie serwera zarządzającego musi odbywać się w pełni automatycznie poprzez administratora, który decyduje kiedy ma ono nastąpić, przełączanie serwera zarządzającego musi być możliwe pomiędzy różnymi typami infrastruktury:
   - serwer fizyczny -> serwer fizyczny

- serwer fizyczny -> serwer wirtualny (onpremis)
- serwer fizyczny -> serwer wirtualny (AWS, Azure, Google)
- serwer wirtualny (onpremis) -> serwer fizyczny
- serwer wirtualny (onpremis) -> serwer wirtualny (onpremis)
- serwer wirtualny (onpremis) -> serwer wirtualny (AWS, Azure, Google)

8. Mechanizm przełączania serwera zarządzającego musi pozwalać (minimum) na wybór trybu:
   - Test failover (testowanie mechanizmu przełączania)
   - Failover (produkcyjne przełączenie działania na serwer standby)
   - Maintenance failover (przełączenie w celu np. aktualizacji oprogramowania)
9. Rozwiązanie musi zapewnić interfejs graficzny do zarządzania i instalacji.
10. Oprogramowanie musi umożliwiać zdalne instalowanie i odinstalowywanie klienta systemu z centralnego serwera dla systemów Windows, Linux i Unix – musi być to możliwe z jednego serwera pełniącego rolę cache dla wszystkich binarii klienckich
11. System musi zapewniać funkcjonalność odtwarzania po awarii konfiguracji serwera zarządzającego tworzeniem kopii bezpieczeństwa i archiwów.
12. System musi posiadać możliwość nieodwracalnego kasowania danych – funkcjonalność ta musi być częścią oprogramowania i musi pozwalać na wyczyszczenie przestrzeni dyskowych (zamazanie) tak aby narzędziami niskiego poziomu nie było możliwości odzyskania tych danych.
13. Administrator systemu musi mieć możliwość wybrania (minimum) plików z danej kopii backupowej i ich skasowania, tak aby nie było możliwości ich późniejszego odtworzenia z tej kopii.
14. Dla dowolnego transferu danych z klienta musi istnieć możliwość definiowania/ograniczania pasma dla transferu danych – funkcjonalność ta musi być dostępna także przy włączonej deduplikacji na kliencie
15. System musi pozwalać na składowanie danych na taśmach celem przechowywania długoterminowego. Składowane dane na taśmach muszą być w formie nie zdeduplikowanej (nawodnione) po to by była możliwość odtwarzania ich bezpośrednio, a więc bez konieczności pośrednictwa dysków, buforów czy importu
16. System musi pozwalać na zarządzanie całością działania systemu (backup, archiwizacja, backup laptopów) z jednej konsoli administracyjnej oraz także z konsoli webowej
17. Agenci systemu muszą posiadać funkcjonalność komunikowania się poprzez jeden port TCP/IP, celem zabezpieczenia komunikacji z środowisk typu DMZ
18. Automatyczne tunelowanie komunikacji TCP/IP pomiędzy agentami systemu – jeśli agent systemu wykryje ograniczenia w komunikacji, wtenczas automatycznie zestawia połączenie tunelowe wykorzystujące tylko jeden port TCP/IP
19. System musi umożliwiać nie tylko szyfrowanie danych (kopii backupowych) ale także całej komunikacji pomiędzy komponentami systemu (minimum pomiędzy agentem backupowym a serwerem składującym i zarządzającym kopiami).

20. System musi umożliwiać konfigurację, którymi kartami sieciowymi ma przebiegać komunikacja i transfer danych, wybór interface musi odbywać się co najmniej poprzez nazwę domeny, subnet, zakres IP
21. System musi pozwalać na współdzielenie napędów taśmowych w środowisku sieci SAN
22. System musi umożliwić przechowywanie jedynie unikalnych bloków danych tzw. deduplikacja. Funkcjonalność ta musi działać na poziomie blokowym i być wykonywana online podczas procesu tworzenia kopii danych. Deduplikacja musi być realizowana poprzez oprogramowanie systemu na dowolnym sprzęcie czy to w warstwie serwera systemu czy klienta. Pojedynczy serwer systemu musi umożliwiać przechowywanie danych po deduplikacji minimum do 500 TB - rozbudowa do tej wielkości może nastąpić tylko poprzez dodanie dodatkowej przestrzeni do składowania danych, poprzez rozbudowę macierzy.
23. Włączenie funkcjonalności deduplikacji na kliencie musi być możliwe dla różnych systemów operacyjnych: Windows, Linux, Unix i Macintosh
24. Logiczna Globalna deduplikacja – system musi oferować deduplikację globalną co oznacza iż niezależnie z jakich klientów dane będą deduplikowane (serwery fizyczne, hosty wirtualne, bazy i aplikację) – deduplikacja musi opierać się na jednej logicznej centralnej bazie deduplikacyjnej
25. Włączenie funkcjonalności deduplikacji nie może generować wymogu instalacji dodatkowych modułów programowych po stronie klienckiej lub serwera systemu.
26. Deduplikacja blokowa musi obejmować dane nie tylko backupowane ale i archiwizowane, przy czym wielkość bloku nie może być większa niż 128KB.
27. System musi zapewniać wspólny stopień deduplikacji (jedna baza deduplikacyjna) dla danych czy to z backupu czy archiwizacji.
28. System musi umożliwiać wykonywanie kopii w post procesie do drugiej lokalizacji przesyłając jedynie unikalne bloki danych (dla dowolnych danych: czy to z procesu backupu czy archiwizacji). A więc replikacja danych do innej lokalizacji musi być wykonywana na danych po deduplikacji i funkcjonalność ta musi być realizowana i zarządzana z poziomu systemu.
29. Replikacja kopii backupowych (tylko unikalne bloki danych po deduplikacji) musi być możliwa w architekturze macierz <-> serwer backupowy, serwer backupowy <-> macierz
30. System musi pozwalać na instalację bazy deduplikacyjnej w układzie wysokiej dostępności (minimum na dwóch serwerach) w taki sposób aby awaria pojedynczego serwera nie powodowała utraty możliwości backupu z deduplikacją i odtwarzania wcześniejszych kopii danych.
31. System musi pozwalać na odtwarzanie zdeduplikowanych danych nawet w momencie, gdy baza deduplikacyjna jest niedostępna. Proces odtwarzania (nawadniania) zdeduplikowanych danych nie korzysta z bazy deduplikacyjnej.
32. System musi zapewniać dostęp zintegrowany z usługą katalogową, minimum to Active Directory, a więc tak zwany „single sign on” – pojedyncze logowanie: użytkownik po zalogowaniu do domeny AD, nie potrzebuje wykonywać następnego logowania aby zarządzać systemem poprzez konsolę administracyjną

33. System musi być odporny na tzw. „atak na wzorzec czasu”: to znaczy iż przy radykalnej zmianie czasu na serwerze zarządzającym System musi automatycznie zatrzymać co najmniej proces kasowania (ekspiracji) kopii backupowych generując odpowiednie alerty do czasu potwierdzenia tej zmiany przez administratora.
34. System musi zapewniać elastyczne delegowanie uprawnień oraz audytowanie działań użytkowników. Z tym, że delegowanie uprawnień musi pozwalać na przydział uprawnień per serwer czy grupa serwerów, przydział uprawnień musi pozwalać na definiowanie uprawnień dla grup użytkowników z domeny AD.
35. System musi pozwalać na zarządzanie z poprzez „cmd” z tym, że uruchomienie jakiejkolwiek komendy/polecenia musi zostać poprzedzone koniecznością zalogowania (autentyfikacji) do systemu, funkcjonalność musi dotyczyć dowolnej platformy (minimum Windows/Linux) i nie może polegać na konieczności instalowania czy konfigurowania dodatkowych komponentów np. SSH.
36. Komunikacja pomiędzy agentem a serwerem systemu musi opierać się na certyfikatach.
37. System musi posiadać funkcjonalność blokowania danych do odczytu dla administratora, to znaczy, że administrator systemu nawet mając pełne uprawnienia nie może odtworzyć danych, jeśli nie jest ich właścicielem, funkcjonalność ta musi być dostępna nie tylko dla danych z laptopów/desktopów ale i dla serwerów (także dla danych plikowych i bazodanowych)
38. System musi pozwalać na skonfigurowanie mechanizmu podwójnej autentyfikacji administratora – do uruchomienia konsoli administracyjnej systemu potrzebne jest nie tylko logowanie, ale i dodatkowy tymczasowy kod wysyłany do administratora np. poprzez mail
39. Szyfrowanie danych musi pozwalać na wybór algorytmu (minimum dwa algorytmy: Blowfish, AES) także dla danych deduplikowanych na kliencie systemu.
40. Możliwość szyfrowania musi pozwalać na elastyczny wybór miejsca szyfrowania: szyfrowanie danych na kliencie, szyfrowanie danych na serwerze backupowym i szyfrowanie tylko transmisji pomiędzy klientem backupowym a serwerem
41. System musi wspierać mechanizm szyfrowania danych na napędach taśmowych LTO
42. System musi pozwalać na ustawianie haseł dostępu do nośników tzw: media password
43. System musi pozwalać na integrację z zewnętrznymi repozytoriami do przechowywania kluczy szyfrującym zgodnymi z KMIP – minimum dla:
    - AWS CloudHSM
    - Fortanix Data Security Manager
    - HashiCorp Vault
    - IBM Security Key Lifecycle Manager (SKLM)
    - Safenet
    - StorMagic SvKMS
    - Thales CipherTrust Manager
    - Vormetric
    - Amazon Web Services (AWS) key management service

- Microsoft Azure Key Vault

44. System musi umożliwiać składowanie kopii bazy katalogowej w chmurze producenta oprogramowania, funkcjonalność ta musi być w cenie produktu i pozwalać na automatyczne składowanie kopii bazy
45. System musi mieć wbudowane mechanizmy zabezpieczające przed złośliwym oprogramowaniem (Ransomware), minimum to:
    - Monitorowanie nietypowych zachować systemu backupowego obejmującego obszary:
    i. Czyszczenia bazy deduplikacyjnej (DDB)
    ii. Zadarzeń w Systemie (events)
    iii. Ilości nieudanych zadań
    iv. Ilości zadań czekających
    v. Ilości zadań zakończonych sukcesem
    vi. Konsoli monitorującej zadania
    vii. Czasu trwania zadań
    - Zabezpieczenie ścieżek dostępu do danych składowanych (kopii backupowych) na dyskach – tylko procesy systemu mogą zapisywać i modyfikować dane
    - Monitorowanie nietypowych aktywności na serwerach plikowych
    - Monitorowanie nietypowych aktywności na serwerach za pomocą metody: Honeypot (plików pułapek/wabików)
    - Monitorowanie możliwego zagrożenia dotyczącego zaszyfrowania plików na serwerach
    - Monitorowanie różnych typów plików i weryfikowanie czy typ pliku jest zgodny i czytelny z nagłówkiem tego pliku (detekcja uszkodzeń plików czy ich zaszyfrowania)
    - Monitorowanie klientów Systemu i alertowanie o tych którzy tracą komunikację z Systemem
    - Air Gap (izolowanie i segmentowanie składowanych kopii backupowych) – musi polegać na wbudowanym automatycznym mechanizmie wyłączania komunikacji pomiędzy pozostałymi komponentami systemu backupowego. Tak więc komunikacja z wybranym segmentem środowiska backupowego odbywa się tylko w określonym przedziale czasowym dla potrzeb replikacji kopii backupowych, natomiast przez pozostały czas żadne procesy systemu backupowego nie mają możliwości komunikacji z tym środowiskiem.
    - Możliwość definiowania serwerów komunikacyjnych (tzw. bram/gateway) przez które wykonywana jest komunikacja pomiędzy modułami systemu backupowego, w szczególności pomiędzy serwerem zarządzającym a serwerem medii czy serwerem z dowolnym agentem backupowym
    - Możliwość definiowania kierunki inicjalizowania komunikacji sieciowej pomiędzy komponentami systemu backupowego
    - Możliwość zablokowania zmiany retencji (czas przechowywania kopii backupowych) na krótszą dla kopii backupowych składowanych na dowolnych typach nośników w tym na dyskach i taśmach

46. System musi posiadać rozbudowany system powiadamiania o zdarzeniach poprzez email.
47. System musi posiadać zaawansowane mechanizmy exportu i analizy logów poprzez:
    - Syslog serwer
    - Splunk (dedykowany plug-in do Spluk dla analizy danych)
48. Automatyczne monitorowanie stanu systemu poprzez wiadomości SMS na urządzeniach mobilnych i telefonach
49. System musi posiadać rozbudowany system raportowania dla administratorów, minimalny zestaw dostępnych raportów to:
    - Raport zmian/wzrostu środowiska systemu
    - Raport wykorzystania licencji
    - Raport wykonanych zadań backupowych
    - Raporty obciążenia serwerów backupowych – minimum monitorowanie użycia CPU i pamięci RAM
50. System musi mieć możliwość automatycznego wysyłania dowolnych raportów do wybranych użytkowników poprzez mail
51. System musi mieć możliwość automatycznego zapisywania raportów w formacie minimum: PDF, HTML i CSV
52. Notyfikacje alertów muszą być wysyłane minimum poprzez mail.
53. Raport spełnienia wymogów SLA dla parametrów:
    - Ilości dodatkowych kopii backupowych
    - RTO
    - RPO
54. System musi zapewniać funkcjonalność wznawiania zadań backupowych.
55. System musi zapewniać funkcjonalność równoległego wykonywania kopii danych backupowanych – inline copy (tego samego zestawu danych pojedynczego klienta) na minimum dwa docelowe urządzenia przechowywania danych.
56. System musi zapewniać funkcjonalność wykonywania zadania backupu wieloma równoległymi strumieniami – tzw. multistreaming. Polega ona na tym iż agent systemu równolegle czyta różne obszary danych i bez pośredniczenia dysków automatycznie wysyła je do serwera, który zapisuje te dane albo na dyski albo na nośniki taśmowe. Funkcjonalność ta musi być dostępna dla dowolnych typów danych: backup plikowy, bazodanowy
57. Funkcjonalność multistreamingu musi być dostępna dla deduplikacji bez względu czy następuje na kliencie czy na serwerze systemu
58. System musi zapewniać funkcjonalność multipleksowania kilku strumieni danych na nośniku taśmowym – tzw. multiplexing. Wydajny zapis wielu strumieni danych na taśmy bez pośrednictwa dysków
59. Rozwiązanie musi posiadać możliwość wykonywania backupu pełnego, przyrostowego, różnicowego oraz syntetycznego.

60. System musi oferować funkcjonalność backupu blokowego, polegającego na tym, iż agent buduje własną bazę zmian bloków danych, przez co backup przyrostowy nie wymaga odczytu całych plików tylko zmienionych bloków wielokrotnie przyspieszając backup. Funkcjonalność ta musi być dostępna dla backupu danych plikowych.
61. System musi posiadać funkcję szyfrowania i kompresji danych transmitowanych przez LAN, możliwość wykorzystania szyfrowania i kompresji musi być dostępna w dowolnej kombinacji.
62. System ma realizować procesy backupu oraz odzyskiwania danych, procesy te muszą być uruchamiane ręcznie i poprzez wbudowany kalendarz, możliwość definiowania zadań poprzez wbudowany w system kalendarz musi być możliwa nie tylko dla zadań backupowych ale także dla zadań odtwarzania danych a więc restore
63. System musi dla backupu środowiska AWS oferować:
    - Bezagentowy backup całych maszyn wirtualnych i ich odtwarzanie wraz z odtwarzaniem pojedynczych plików
    - Możliwość zapisu backupu maszyn wirtualnych na dowolnym nośniku backupowym.
    - Możliwość odtworzenia pojedynczego dysku wirtualnej maszyny i podłączenie go do innej maszyny wirtualnej EC2
    - Możliwość wykonywania migawek (snapshotów) wirtualnych maszyn i automatyczne zarządzanie ich retencją
    - Możliwość wykonywania jednoprzebiegowego konsystentnego backupu maszyn wirtualnych EC2, na których pracują systemy Microsoft Exchange, Microsoft Sharepoint, Microsoft SQL Server, MySQL, Oracle lub Active Directory
    - Backup i odtwarzanie danych z baz danych RDS: MS SQL, MySQL, PostgreSQL oraz Oracle (eksport danych na storage backupowy)
    - Możliwość wykonywania snapshotów baz danych AWS RDS: Aurora, MariaDB, Microsoft SQL Server, MySQL, PostgreSQL.
    - Backup oraz odtwarzanie danych składowanych w usłudze S3, EFS oraz FSx.
    - Możliwość zapisu danych zdeduplikowanych bezpośrednio w usłudze S3, bez konieczności używania dodatkowego cache'u oraz rozwiązan typu appliance
    - Możliwość automatycznego włączania oraz wyłączania maszyn wirtualnych EC2, na których zainstalowano oprogramowanie serwera backupowego
    - Możliwość konwersji maszyn wirtualnych Microsoft Hyper-V, Vmware oraz Azure do maszyn wirtualnych EC2
    - Możliwość konwersji maszyn wirtualnych EC2 do maszyn typu Vmware oraz Azure
    - Możliwość wykonywania backupu usługi AWS DynamoDB
    - Możliwość backupu środowiska VMWare Cloud on AWS
    - Możliwość automatycznego wyłączania i włączania serwerów backupowych
    - Możliwość automatycznej replikacji maszyn wirtualnych Vmware do AWS EC2

- Możliwość wykorzystania EBS Direct Read API w czasie backupu maszyn wirtualnych EC2
- Możliwość integracji z AWS KMS w celu zarządzania kluczami szyfrującymi
- Możliwość backupu maszyn wirtualnych EC2 z innego konta Amazon (Cross-account backup)
- Możliwość migracji zdeduplikowanych danych do chmury AWS za pomocą urządzenia Snowball
- Możliwość wykonywania konsystentnych snapshotów dysków wirtualnych podłączonych do maszyn wirtualnych Azure VM, na których składowane są dane systemów Oracle, SAP HANA, Microsoft SQL Server, DB2, MongoDB, MySQL, PostgreSQL oraz pliki na systemach Windows oraz Linux

64. System musi dla backupu środowiska Azure oferować:
    - Bezagentowy backup całych maszyn wirtualnych Azure VM i ich odtwarzanie wraz z odtwarzaniem pojedynczych plików.
    - Możliwość zapisu backupu maszyn wirtualnych na dowolnym nośniku backupowym.
    - Możliwość odtworzenia pojedynczego dysku wirtualnej maszyny i podłączenie go do innej maszyny wirtualnej w Azure VM
    - Możliwość wykonywania migawek (snapshotów) wirtualnych maszyn i automatyczne zarządzanie ich retencją
    - Możliwość wykonywania jednoprzebiegowego konsystentnego backupu maszyn wirtualnych Azure VM, na których pracują systemy Microsoft Exchange, Microsoft Sharepoint, Microsoft SQL Server, MySQL, Oracle lub Active Directory
    - Backup i odtwarzanie danych z baz danych (PaaS): MS SQL, MySQL, PostgreSQL (eksport danych na storage backupowy)
    - Backup oraz odtwarzanie danych składowanych w Azure Blob oraz Azure File Shares oraz Azure Data Lake Storage Gen2
    - Możliwość zapisu danych zdeduplikowanych bezpośrednio na Azure Blob Storage, bez konieczności używania dodatkowego cache'u oraz rozwiązan typu appliance
    - Możliwość automatycznego włączania oraz wyłączania maszyn wirtualnych Azure, na których zainstalowano oprogramowanie serwera backupowego
    - Możlwość wykonywania konsystentnych snapshotów dysków wirtualnych podłączonych do maszyn wirtualnych Azure VM, na których składowane są dane systemów Oracle, SAP for Oracle, SAP HANA, Microsoft SQL Server, DB2 oraz pliki na systemach Windows oraz Linux
    - Możliwość migracji zdeduplikowanych danych do chmury Azure za pomocą Azure Data Box
    - Możliwość automatycznego wyłączania i włączania serwerów backupowych
    - Możliwość integracji z Azure Key Vault w celu zarządzania kluczami szyfrującymi
    - Możliwość automatycznej replikacji maszyn wirtualnych Hyper-V i Vmware do Azure
    - Możliwość automatycznej replikacji maszyn wirtualnych Azure pomiędzy regionami

- Możliwość backupu bazy danych Cosmos DB (Core SQL API)
- Możliwość konwersji backupu systemu operacyjnego Windows wraz z danymi do maszyny wirtualnej Azure
- Możliwość backupu Azure DevOps and GitHub

65. System musi dla backupu środowiska GCP oferować
    - Bezagentowy backup całych maszyn wirtualnych i ich odtwarzanie wraz z odtwarzaniem pojedynczych plików
    - Możliwość zapisu backupu maszyn wirtualnych na dowolnym nośniku backupowym.
    - Możliwość wykonywania migawek (snapshotów) wirtualnych maszyn i automatyczne zarządzanie ich retencją
    - Backup i odtwarzanie danych z baz danych Cloud SQL: MySQL oraz PostgreSQL (eksport danych na dowolny storage backupowy)
    - Backup oraz odtwarzanie danych składowanych w usłudze GCP Cloud Storage
    - Możliwość zapisu danych zdeduplikowanych bezpośrednio w usłudze GCP Cloud Storage, bez konieczności używania dodatkowego cache'u oraz rozwiązan typu appliance
66. System musi posiadać (jako opcja) zintegrowane w systemie mechanizmy indeksowania pełnokontekstowego i wyszukiwania danych. Indeksowaniu powinny podlegać dane zbackupowane i zarchiwizowane już znajdujące się w systemie.
67. System musi realizować funkcjonalność weryfikacji wykonanych kopii.
68. System powinien umożliwiać wykorzystanie funkcjonalności Bare Metal Restore dla odtwarzania systemu po awarii, wsparcie musi być dostępne dla systemów:
    - Windows
    - Linux: Debian/Oracle Linux/RHEL/CentOs/SuSe/Ubuntu
69. System musi umożliwiać integrację z mechanizmami kopii migawkowych czołowych producentów pamięci masowych minimum: HDS, Dell, HP, NetApp, EMC, IBM, Pure Storage z tym że takowy backup sterowany przez system a wykonywany przez daną macierz dyskową musi być dostępny nie tylko dla zasobów plikowych ale i aplikacji.
70. Dla producentów: NetApp, EMC i HDS system musi umożliwiać nie tylko integrację z mechanizmami tworzenia kopii migawkowych (tzw. Snapshot) ale musi integrować się także z mechanizmami replikacyjnymi, a więc sterować replikami wykonywanymi przez macierze
71. System powinien umożliwiać składowanie kopii backupowych na storage obiektowym w chmurze, minimum: Azure, Amazon, Google Cloud, jeśli do włączenia tej funkcjonalności potrzebne są jakieś dodatkowe komponenty to muszą być zaoferowane
72. System musi umożliwiać backup danych z zasobów obiektowych czy to chmurowych (minimum: AWS, Azure, Google, OCI czy onpremis (minimum: Red Hat Ceph Storage, Pure Storage FlashBlade)
73. System musi umożliwiać odtwarzanie danych plikowych pomiędzy systemami operacyjnymi np. odtwarzanie danych plikowych Linux na systemie Windows

74. System musi pozwalać na odtwarzanie tylko samych uprawnień do plików
75. System musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL)
76. System musi posiadać wbudowany mechanizm tworzenia kopii otwartych plików na platformie Windows
77. System musi wspierać wykonanie kopii na systemach klasy Windows, Linux i Unix
78. System musi posiadać szerokie wsparcie dla środowisk Linux, minimum: RHEL, SuSe, Debian, Fedora, Gentoo, Oracle Linux, Scientific Linux, Ubuntu, Slackware
79. System musi posiadać szerokie wsparcie dla środowisk Unix, minimum: AIX, FreeBSD, HP-UX, Solaris
80. System musi umożliwiać uruchamianie skryptów przed i po backupie, z tym iż musi posiadać mechanizm definiowania konta użytkownika na którym te skrypty byłyby uruchamiane. Mechanizm ten musi być centralnie zarządzany poprzez konsolę administracyjną. Niedopuszczalna jest konieczność np. zmiany konta serwisowego dla danego agenta – konta serwisowe muszą być centralnie definiowane i zarządzane.
81. System musi wspierać backup całych maszyn wirtualnych/kontenerów dla czołowych rozwiązań wirtualizacyjnych, kontenerowych i chmurowych:
    - Alibaba Cloud
    - Amazon
    - Citrix Xen
    - Google Cloud Platform
    - Huawei FusionCompute
    - Microsoft Azure
    - Microsoft Azure Stack Hub
    - Microsoft Azure Stack HCI
    - Microsoft Hyper-V
    - Kubernetes
    - Nutanix Acropolis Hypervisor (AHV)
    - OpenStack
    - Oracle Cloud Classic
    - Oracle Cloud Infrastructure
    - Oracle VM
    - Red Hat OpenShift
    - Red Hat Virtualization
    - vCloud Director
    - VMware

    To znaczy musi posiadać dedykowany komponent do backupu minimum całej maszyny wirtualnej/kontenera/aplikacji/wolumenu bez konieczności instalowania agenta wewnątrz np. maszyny

z możliwością granualnego odtwarzania pojedynczych plików. Dla maszyn wirtualnych musi być możliwość zainstalowania agenta plikowego i bazodanowego dla zabezpieczenia zasobów z wewnątrz maszyny wirtualnej – funkcjonalność ta musi być zawarta dla wszystkich wymaganach wirtualizatorów i być w cenie rozwiązania.

82. System musi wspierać wersje środowisk VMware 4.1, 5.0.x, 5.1.x, 5.5, 5.5.1, 5.5.2, 5.5.3, 6.0, 6.0.1, 6.5, 6.7, 7.0,7.0.3, 8.0 poprzez integrację z vStorage API
83. Dla backupu i odtwarzania środowisk wirtualnych opartych o Vmware musi być możliwość wyboru różnych transportów: SAN, Hot-add, NBD, SSL, NAS - gdzie transport NAS pozwala na bezpośredni odczyt i zapis danych maszyny wirtualnej z urządzenia NAS
84. System musi wspierać środowisko Hyper-V.
85. System musi zapewniać automatyczne wykrywanie i dodawanie do polityki backupu nowych maszyn wirtualnych.
86. System musi umożliwiać odzyskanie i uruchomienie maszyn wirtualnych z kopii zapasowej bez oczekiwania na pełne przywrócenie maszyny wirtualnej minimum dla Vmware i Hyper-V.
87. System musi umożliwiać konwertowanie maszyn wirtualnych pomiędzy wirtualizatorami, minimum:
    - Vmware do: Hyper-V, Azure, Amazon, Google Cloud Platform, Openstack, Oracle Cloud Infrastructure
    - Hyper-V do: Azure, Amazon, Vmware
    - Amazon do: Azure, Vmware
    - Azure do: Amazon, Hyper-V, Vmware
88. System musi wspierać mechanizm CBT (change block tracking) minimum dla Vmware i Hyper-V
89. System musi umożliwiać konwersję zbackupowanego serwera Windows i Linux do maszyny wirtualnej w środowisku:
    - Hyper-V
    - Vmware
90. Możliwość (jako opcja) synchronizacji maszyn wirtualnych Vmware do środowiska Amazon, Azure
91. System musi umożliwiać wykonanie kopii na gorąco bazy danych MySQL, Postgress, Oracle, Informix na dowolnej platformie systemu operacyjnego (Windows/Linux/Unix) poprzez dedykowanego agenta bazodanowego, transfer danych musi odbywać się bez pośredniczenia dysków, a więc transfer danych z agenta bazodanowego bezpośrednio do serwera backupowego celem zapisu na dany nośnik.
92. System musi umożliwiać wykonanie kopii na gorąco bazy danych MS SQL, Oracle, MySQL, Postgress, DB2, Informix konfiguracja agenta nie może powodować konieczności tworzenia skryptów uruchamianych po stronie klienta niezależnie czy jest to serwer fizyczny czy wirtualny. Brak skryptów musi dotyczyć dowolnych typów backupów: backup automatyczny uruchamiany poprzez harmonogram, backup manualny.

93. Odtwarzanie danych z backupu bazodanowego (MS SQL, Oracle, MySQL, Postgress, DB2, Informix) musi odbywać się poprzez konsolę administracyjną bez konieczności konfigurowania skryptów.
94. Dla silników bazodanowych MS SQL, Oracle i SAP HANA musi istnieć mechanizm backupu logów tranzakcyjnych z częstotliwością co 1 minuta nawet w przypadku gdy serwer zarządzający systemem backupowym jest niedostępny
95. Konfiguracja agentów backupowych dla: MS SQL, Oracle, mySQL musi odbywać się poprzez interface graficzny, jakakolwiek modyfikacja zasobów do backupu (np. dodanie nowej bazy) nie może powodować konieczności modyfikacji skryptów czy to dla backupów planowanych czy wykonywanych na żądanie
96. System musi umożliwiać wykonanie kopii na gorąco Active Directory a następnie odzyskania pojedynczych obiektów AD wraz z hasłami użytkowników
97. System musi umożliwiać odtwarzanie backupu wykonywanego online dedykowanym agentem, do pliku celem późniejszego odtwarzania bez udziały systemu. Funkcjonalność ta musi być dostępna minimum dla MS SQL, Oracle i Exchange
98. System musi umożliwiać wykonanie kopii na gorąco aplikacji MS Exchange a następnie odzyskania pojedynczych wiadomości. Dedykowany agent do backupu Exchange musi wspierać backup środowiska Exchange DAG poprzez nazwę DAG nawet w konfiguracji bez adresu IP
99. System musi umożliwiać odtwarzanie pojedynczych tabel dla minimum: Oracle, DB2, PostgreSQL, MySQL, Informix, MS SQL
100. Dla minimum mySQL i PostgresSQL musi istnieć mechanizm backupu z wykorzystaniem mechanizmu backupu blokowego
101. Automatyczny backup logów transakcyjnych dla baz danych w oparciu o procent wolnego miejsca na systemie plikowym, minimum dla: Oracle, SQL, Notes, SAP/Oracle
102. Dla MS SQL możliwość skonfigurowania rozszerzenia pozwalającego backupować i odtwarzać bazy bezpośrednio z konsoli Management Studio
103. Wsparcie dla backupu online dla minimum MS SQL Server 2005/2008/2008 R2/2012/2014/2016/2017/2019/2022 na platformie Windows
104. Dedykowany agent bazodanowy dla backupu MS SQL (2017/2019/2022) na platformie Linux: Ubuntu, SuSe, RHEL
105. Odtwarzanie baz SAP opartej na silniku Oracle do pliku, a więc odtwarzanie backupu online na dysk (tzw. application free restore)
106. Dedykowani agenci do backupu systemów Big Data: Hadoop, Greenplum, GPFS, Splunk, MongoDB
107. Możliwość integracji kopii migawkowych dla backupu konsystentnego aplikacji i baz danych minimum: Vmware, Hyper-V, MS SQL, Exchange, mySQL, Oracle – zarządzanie kopiami migawkowymi musi odbywać się z konsoli administracyjnej systemu backupowego a integracja zarządzania nie może odbywać się na bazie skryptów

108. Możliwość (jako opcja) pełnokontekstowego indeksowania i wyszukiwania treści (eDiscovery i Compliance Search) z danych backupowanych z:
    - Skrzynek pocztowych (Exchange onpremis)
    - Skrzynek journalingowych (Exchange onpremis)
    - Ruchu pocztowego SMTP
    - Exchange Online
    - Serwerów plikowych
    - Laptopów i desktopów
    - OneDrive for Business
    - SharePoint Online
109. Możliwość backupu (jako opcja) danych z aplikacji Salesforce, minimalny zakres backupowanych danych to:
    - Standard objects
    - Custom objects
    - Dokumenty
    - Załączniki
    - CRM content
    - Pliki
110. System musi zapewniać (jako opcja) backup laptopów i desktopów – funkcjonalność ta musi być w pełni zintegrowana z systemem (ta sama konsola, to samo repozytorium danych, ta sama deduplikacja) o funkcjonalnościach:
    - Portal samoobsługowy musi być dostępny poprzez dowolną przeglądarkę sieci Internet minimum: Edge, Chrome, Opera, Mozilla, Safari
    - System musi umożliwiać backup laptopów czy desktopów z systemami Windows, Linux i Macintosh
    - Dostęp do danych zbackupowanych z laptopów czy desktopów musi być możliwy z urządzeń mobilnych poprzez dedykowanego klienta minimum dla IOS i Android
    - Dla backupu laptopów i desktopów system backupowy musi oferować dedykowanego agenta, który pozwala skonfigurować zadanie backupowe tak by było wykonane w przedziale czasowym bez podawania konkretnej daty czy czasu jego uruchomienia, agent nie może tworzyć kopii danych na lokalnych zasobach stacji/laptopa.
    - System musi zapewniać współdzielenie plików pochodzących z backupu laptopów i destopów z użytkownikami z domeny AD oraz z użytkownikami spoza domeny.
    - Każdy użytkownik desktopa czy laptopa musi posiadać możliwość zarządzania własnymi danymi, minimalna oczekiwana funkcjonalność to:
        - ✓ Odtwarzanie własnych danych
        - ✓ Uruchomienie backupu

- ✓ Wstrzymanie backupu
- ✓ Możliwość zdefiniowania innego okna backupowego
- ✓ Możliwość monitorowania postępu działania zadania
- ✓ Możliwość przeglądania danych z stacji roboczej czy laptopa poprzez dedykowanego klienta dla urządzeń mobilnych, a więc użytkownik posiadając jedynie urządzenie mobilne może nie tylko odczytywać dane z backupowej kopii ale także przeglądać dane na stacji roboczej nawet w momencie gdy jest poza siedzibą firmy – korzysta jedynie z dostępu do internetu (do przeglądania danych nie jest potrzebne żadne dodatkowe połączenie VPN)

- Zabezpieczenie przed kradzieżą, system musi posiadać możliwość zdalnego zaszyfrowania danych w przypadku kradzieży laptopa, to znaczy iż w przypadku utraty urządzenia administrator lub użytkownik włącza opcję szyfrującą i jeśli urządzenie pojawi się w sieci wtenczas automatycznie dane zostaną zaszyfrowane
- Możliwość archiwizowania danych plikowych na stacji roboczej: jeśli dane pliki spełniają kryteria archiwizacyjne to dany pliki zostaje skasowany albo zamieniony na skrót (stub)

111. Rozwiązanie musi pozwalać na archiwizację danych z możliwością pozostawiania znaczników (stub) na zasobach produkcyjnych (dla zasobów plikowych Windows\Linux\Unix) serwerów fizycznych, archiwizacja musi korzystać z tej samej architektury systemu co backup i korzystać z tego samego repozytorium danych.

112. System musi posiadać funkcjonalności archiwizacyjne (archiwizacja plikowa) takie jak:

- Oprogramowanie musi wspierać archiwizację zgodnych z wyznaczonymi kryteriami danych z systemów produkcyjnych na inne tańsze pamięci masowe. Mechanizm ten pozwoli na zmniejszenie ilości danych na systemach produkcyjnych.
- Oprogramowanie musi być zintegrowane z modułem do tworzenie kopii zapasowych w celu redukcji czasu okien backupowych przy zabezpieczaniu dużej ilości danych.
- Oprogramowanie musi umożliwiać deduplikację danych archiwizowanych na poziomie bloków w celu redukcji ilości przestrzeni na dyskach fizycznych. Oprogramowanie musi umożliwiać globalną deduplikację dla archiwizacji i kopii zapasowych w celu minimalizowania zużycia pamięci masowej.
- Oprogramowanie musi zapewniać przezroczysty dostęp użytkowników do danych archiwalnych poprzez mechanizm skrótów

113. System musi (jako opcja) umożliwiać rozbudowę o archiwizację poczty (minimum Exchange), archiwizacja poczty musi umożliwiać archiwizowanie maili z skrzynek pocztowych oraz archiwizowanie ruchu pocztowego (journaling lub SMTP journaling)

114. System musi oferować mechanizm składowania kopii backupowych (retencja danych) oparty o czas i cykle. Oznacza to iż kopia backupowa jest przechowywana w repozytorium przez okre-

ślony czas (np. tydzień, miesiąc, rok….) a jej automatyczne skasowanie jest wykonane jeśli spełniony jest jednocześnie warunek ilości cykli a więc ilość backupów typu pełnego lub backupów syntetycznych znajdujących się w systemie

115. System musi oferować integrację z mechanizmami deduplikacyjnymi urządzeń typu appliance minimalne wsparcie to Catalyst i urządzenie StoreOnce. Integracja z StoreOnce musi być dostępna nie tylko dla Windows ale także dla Unix i Linux.
116. System (jako opcja) musi oferować rozbudowę o funkcjonalność przeszukiwania i analizy zasobów plikowych dla maszyn wirtualnych (minimum Vmware) całość działać związanych musi odbywać się na kopiach backupowych maszyn wirtualnych a nie na środowisku produkcyjnym
117. System (jako opcja) musi posiadać zaawansowaną funkcjonalność analizy zasobów plikowych minimum o funkcjonalnościach:
    - Detekcja powtarzających się zasobów
    - Raportowanie praw dostępu do plików
    - Raportowanie i analiza dostępu do zasobów i ich modyfikacji
    - Możliwość kasowania plików z zasobów produkcyjnych
118. System (jako opcja) musi pozwalać na wyszukiwanie danych wrażliwych (np. numery PESEL) i pozwalać osobie uprawnionej nie tylko na raportowanie takich zdarzeń ale także umożliwiać kasowanie plików nie tylko z systemów produkcyjnych ale i z kopii backupowej
119. Musi istnieć możliwość zarządzania systemem poprzez Windows PowerShell
120. Agent do spójnego backupu bazy HBASE – backup pełny i przyrostowy
121. Agent do backupu systemów plikowych: Lustre, GlusterFS
122. System musi zamierać moduł do monitorowania i zarządzania taśmami wynoszonymi z bibliotek taśmowych o funkcjonalnościami minimum:
    - Identyfikacja taśm, które muszą być wyciągnięte z biblioteki
    - Identyfikacja taśm, które można z powrotem wstawić do biblioteki taśmowej
    - Automatyczne przenoszenie taśm w bibliotece i notyfikacja administratorów
    - Identyfikacja i monitorowanie nośników (taśm) w trakcie transportu
123. Możliwość backupu baz Oracle bez instalacji oprogramowania backupowego natomiast dane zbackupowane muszą być składowane i zarządzane przez system backupowy
124. System musi posiadać integrację z ServiceNow o funkcjonalnościach:
    - Dedykowany plugin do ServiceNow
    - Możliwość zgłaszania zdarzeń backupowych i odtworzeniowych bezpośrednio z konsoli ServiceNow
125. Możliwość (jako opcja) rozbudowy środowiska o moduł VTL dla backupu danych po sieci SAN i LAN na dowolnym sprzęcie typu x86
126. Możliwość włączenia backupu pojedynczego pliku wieloma strumieniami
127. Możliwość zwiększenia bezpieczeństwa systemu poprzez integrację z CyberArk

128. Musi istnieć możliwość wskazania klucza szyfrującego (Bring Your Own Key – BYOK), który będzie wykorzystywany do szyfrowania kopii backupowych
129. Dedykowane moduły do integracji z Terraform
130. Możliwość anonimizacji danych wrażliwych (data masking) minimum dla logów systemu wysyłanych np. do wsparcia
131. Podstawowe komponenty systemu jak: serwer zarządzający, serwery składujące i deduplikujące dane muszą wspierać system operacyjny Linux, a więc musi istnieć możliwość bezpośredniego zainstalowania na systemie Linux tych komponentów bez jakiejkolwiek warstwy wirtualizacyjnej.

3.2.12.3. **Wymogi dla licencjonowania (licencjonowanie typu perpertual)**

1. Wszystkie potrzebne licencje dla zbudowania rozwiązania backupowego musi być zaoferowane w modelu perpertual, dotyczy to sprzętu, storage, systemu operacyjnego i oprogramowania backupowego.
2. Licencjonowanie dt. sprzętu i licencjonowanie samego oprogramowania backupowego musza być rozdzielne i niezależne tak aby możliwa była rozbudowa czy to sprzętu czy samych licencji backupowych.
3. Wszelkie możliwe rozbudowy funkcjonalności backupowych np. o backup O365 muszą być licencjonowane także w modelu perpertual.
4. Niedopuszczalne jest aby licencjonowanie oprogramowania backupowego było zależne od ilości składowanych danych (kopii backupowych) na dowolnych nośnikach (np. dysk, taśma VTL…) czy to z deduplikacją czy bez.
5. Niedopuszczalne jest aby licencjonowanie oprogramowania backupowego było zależne od ilości komponentów środowiska backupowego, które będą wykorzystywane w procesie backupu czy odtwarzania danych.
6. Niedopuszczalne jest aby licencjonowanie zależne było od ilości serwerów fizycznych czy ich mocy (ilości procesorów) niezależnie czy dane są z nich backupowane bezpośrednio czy tworzą platformę wirtualizacyjną, która jest backupowana.
7. Zaoferowane licencje oprogramowania backupowego nie mogą ograniczać wielkości przestrzeni do składowania danych czy replik ich do innych lokalizacji.
8. Oferowana licencja oraz architektura systemu musi pozwalać na backup danych na:
   a. nielimitowana ilość bibliotek taśmowych i napędów taśmowych
   b. nielimitowaną przestrzeń w rozwiązaniach chmurowych (minimum: AWS, Azure, Google)
9. Zaoferowane licencje nie mogą mieć żadnych ograniczeń czasowych (muszą być wieczyste) dla wszystkich wymaganych funkcjonalności backupowych oraz sprzętu.
10. Do dostarczonych licencji jest wymagane 36 miesięczne wparcie producenta lub autoryzowanego partnera serwisowego (pierwsza i druga linia wsparcia świadczona w języku polskim lub

angielskim) zapewniające wsparcie techniczne w trybie 24/7/265 oraz dostęp do bezpłatnych ewentualnych poprawek i uaktualnień.

11. Zaoferowane licencje na system muszą zapewnić backup danych z środowiska o wielkości:
    a. środowisko serwerów fizycznych i NAS wraz z aplikacjami i bazami - 30 TB (Front End).

3.2.12.4. Wymogi dla urządzeń wchodzących w skład systemu backupu

3.2.12.4.1. Ogólne

Wykonawca zobowiązany jest dostarczyć dwa serwery, z których jeden będzie wykorzystany jako serwer backupu (serwer zarządzający) a drugi będzie pełnił rolę serwer proxy/media agent tj. będzie pośredniczył w transferze danych z serwerów produkcyjnych na macierz backupową (serwer przechowywania i transferu danych).
Kopie backupowe muszą być składowane na macierzy dyskowej prezentującej dane po protokole CIFS lub NFS. Dane na macierzy muszą być zabezpieczone przez odpowiedni mechanizm RAID.
Minimalna przestrzeń netto dla składowania kopii backupowych po deduplikacji na macierzy dyskowej to 87TB.
Zamawiający nie dopuszcza składowania danych na wewnętrznych dyskach serwerów.
Inicjalna konfiguracja systemu powinna zapewniać skalowalność do 150 danych po deduplikacji jedynie poprzez rozbudowę przestrzeni dyskowej macierzy, bez konieczności modyfikacji parametrów serwerów backupu.
Podstawowe komponenty systemu backupowego (w tym min. serwer zarządzający backupem) muszą być zainstalowane i skonfigurowane na serwerze backupu. Wymagane jest aby serwer backupu posiadał możliwość pracy w trybie active/standby z serwerem backupu zlokalizowanym w ośrodku zapasowym po rozbudowie systemu o drugi ośrodek przetwarzania.
Rozwiązanie musi mieć możliwość skalowania pojedynczej puli deduplikacyjnej do 1 PB poprzez dodanie nowych serwerów proxy/media agent oraz rozbudowę przestrzeni dyskowej macierzy.
Wszelkie licencje na systemy operacyjne potrzebne dla uruchomienia systemu backupowego muszą być dostarczone wraz z serwerami.
Monitorowanie stanu serwerów i macierzy dostarczanych na potrzeby backupu musi odbywać się z poziomu oprogramowania do zarządzania serwerami i macierzami.
System musi mieć możliwość włączenia Immutable Storage zwiększające bezpieczeństwo składowania kopii backupowych poprzez wykorzystanie funkcjonalności:

- Retention Lock (WORM)
- Ransomware Protection
- Onboard Firewall

3.2.12.4.2. Wymagania dla serwera backupu – 1 szt.

Lp.	Element/cecha/komponent	Wymagania minimalne
1	Obudowa	Wysokość maksymalnie 1U, przystosowana do montażu w szafie stelażowej 19 cali (wraz ze wszystkimi elementami niezbędnymi do zamontowania serwera w szafie stelażowej z możliwością wysunięcia bez konieczności odłączania okablowania).
2	Procesor	Minimalna częstotliwość bazowa rdzeni procesora zamontowanego w serwerze to 3,2 GHz, minimalna sumaryczna ilość rdzeni procesora zamontowanego w serwerze to 16 szt. Procesor osiągający w testach „SPECint_rate2017 Baseline" wynik nie gorszy niż 135 pkt. Wynik testu musi dotyczyć oferowanego serwera.
3	Pamięć operacyjna	Minimum 64 GB DDR5 z ochroną pamięci ECC. Pamięci w oferowanej konfiguracji muszą pracować z szybkością transmisji danych nie niższą niż 4800MHz. Użyte kości pamięci muszą być jednakowe (model, rozmiar, typ). Serwer musi posiadać min. 32 gniazda pamięci RAM DDR5.
4	Gniazda rozszerzeń	Łącznie minimum 2 gniazda PCI Express czwartej generacji. Minimum 1 gniazdo OCP 3.0
5	Dysk twardy	Serwer musi być wyposażony w minimum 2 szt. dysków SSD 480 GB, 2,5" SAS/SATA/U.2 Hot Plug, Read Intensive oraz 2 szt. dysków SSD 480 GB, 2,5" SAS/SATA/U.2 Hot Plug, Mixed Use zamontowane w wewnętrznych kieszeniach serwera. Serwer musi być wyposażony w kontroler sprzętowy. zapewniający RAID 1, 10, 5 dla ww. dysków. Serwer musi zapewniać możliwość rozbudowy do minimum 8 szt. dysków (bez konieczności dokładania dodatkowych elementów). Wszystkie urządzenia muszą być zamontowane wewnątrz obudowy serwera, kompatybilne z systemem wirtualizacji dostarczanym w ramach niniejszego zamówienia.

6	Karty sieciowe	Minimum 4 szt. portów pracujących z minimalną prędkością 25 GbE, wyposażonych we wkładki SFP28.
8	Karta graficzna	Zintegrowana karta graficzna do obsługi wyjścia wideo
9	Porty	Minimum 1 dodatkowy port RJ-45 dedykowany dla interfejsu zdalnego zarządzania, minimum 2 x USB zewnętrzne. Nie dopuszcza się stosowania spliterów oraz kart zajmujących wolne sloty PCIe w serwerze w celu osiągnięcia wymaganej liczby portów USB; minimum 1x VGA.
10	Zasilacz	Minimum dwa zasilacze wyposażone w złącza C13 hotplug, zapewniające redundancję zasilania na poziomie N+N. Połowa spośród zainstalowanych zasilaczy musi zapewniać możliwość zasilenia serwera, przy zachowaniu jego pełnych możliwości operacyjnych umożliwiających pracę z maksymalną wydajnością podczas pracy ciągłej.
11	Chłodzenie	Zestaw wentylatorów zapewniających redundantne chłodzenie serwera, typu hot-plug. Serwer musi zapewnić stabilne działanie przy temperaturze otoczenia co najmniej 25 st. C.
12	Wspierane systemy operacyjne i wirtualizacyjne	MS Windows Server 2022 lub nowsze wersje Red Hat Enterprise Linux 8.X lub nowsze wersje, VMware ESX 7.x lub nowsze wersje lub równoważne
13	Instalacja	Instalacja i konfiguracja serwera wykonana przez inżyniera producenta serwera

3.2.12.4.3. Wymagania dla serwera proxy\media agent – 1 szt.

Lp.	**Element/cecha/komponent**	**Wymagania minimalne**
1	Obudowa	Wysokość maksymalnie 1U, przystosowana do montażu w szafie stelażowej 19 cali (wraz ze wszystkimi elementami niezbędnymi do zamontowania serwera w szafie stelażowej z możliwością wysunięcia bez konieczności odłączania okablowania).
2	Procesor	Minimalna częstotliwość bazowa rdzeni procesora zamontowanego w serwerze to 3,2 GHz, minimalna sumaryczna ilość rdzeni procesora zamontowanego w serwerze to 16

		szt. Procesor osiągający w testach „SPECint_rate2017 Baseline” wynik nie gorszy niż 135 pkt. Wynik testu musi dotyczyć oferowanego serwera.
3	Pamięć operacyjna	Minimum 128 GB DDR5 z ochroną pamięci ECC. Pamięci w oferowanej konfiguracji muszą pracować z szybkością transmisji danych nie niższą niż 4800MHz. Użyte kości pamięci muszą być jednakowe (model, rozmiar, typ). Serwer musi posiadać min. 32 gniazda pamięci RAM DDR5.
4	Gniazda rozszerzeń	Łącznie minimum 2 gniazda PCI Express czwartej generacji. Minimum 1 gniazdo OCP 3.0
5	Dysk twardy	Serwer musi być wyposażony w minimum 2 szt. dysków SSD 480 GB, 2,5” SAS/SATA/U.2 Hot Plug, Read Intensive oraz 4 szt. dysków SSD 1,92 TB, 2,5” SAS/SATA/U.2 Hot Plug, Mixed Use zamontowane w wewnętrznych kieszeniach serwera. Serwer musi być wyposażony w kontroler sprzętowy wyposażony w 2 GB pamięci cache. zapewniający RAID 1, 10, 5 oraz 6 dla ww. dysków. Serwer musi zapewniać możliwość rozbudowy do minimum 8 szt. dysków (bez konieczności dokładania dodatkowych elementów). Wszystkie urządzenia muszą być zamontowane wewnątrz obudowy serwera, kompatybilne z systemem wirtualizacji dostarczanym w ramach niniejszego zamówienia.
6	Karty sieciowe	Minimum 4 szt. portów pracujących z minimalną prędkością 25 GbE, wyposażonych we wkładki SFP28.
8	Karta graficzna	Zintegrowana karta graficzna do obsługi wyjścia wideo
9	Porty	Minimum 1 dodatkowy port RJ-45 dedykowany dla interfejsu zdalnego zarządzania, minimum 2 x USB zewnętrzne. Nie dopuszcza się stosowania spliterów oraz kart zajmujących wolne sloty PCIe w serwerze w celu osiągnięcia wymaganej liczby portów USB; minimum 1x VGA.
10	Zasilacz	Minimum dwa zasilacze wyposażone w złącza C13 hotplug, zapewniające redundancję zasilania na poziomie N+N. Połowa spośród zainstalowanych zasilaczy musi zapewniać możliwość zasilenia serwera, przy zachowaniu jego pełnych możliwości operacyjnych umożliwiających pracę z maksymalną wydajnością podczas pracy ciągłej.

11	Chłodzenie	Zestaw wentylatorów zapewniających redundantne chłodzenie serwera, typu hot-plug. Serwer musi zapewnić stabilne działanie przy temperaturze otoczenia co najmniej 25 st. C.
12	Wspierane systemy operacyjne i wirtualizacyjne	MS Windows Server 2022 lub nowsze wersje Red Hat Enterprise Linux 8.X lub nowsze wersje, VMware ESX 7.x lub nowsze wersje lub równoważne
13	Instalacja	Instalacja i konfiguracja serwera wykonana przez inżyniera producenta serwera

3.2.12.4.4. Wymagania dla macierzy backup – 1 szt.

Lp.	Element/cecha/komponent	Wymagania minimalne
1	Dokumentacja producenta	Każda funkcjonalność wyspecyfikowana w dokumencie musi mieć potwierdzenie w aktualnym oraz ogólnodostępnym dokumencie producenta w postaci instrukcji użytkownika lub dokumentacji technicznej. W razie wątpliwości co do realizacji funkcjonalności, Zamawiający może zwrócić się do oferenta o udostępnienie wyżej wymienionych dokumentów w celu potwierdzenia jej realizacji.
2	Standard RACK	Wymagane jest rozwiązanie mieszczące się w standardowej, pojedynczej szafie 19” 42U, niededykowanej wyłącznie dla macierzy. Preferowane jest rozwiązanie kompaktowe tj. o jak najmniejszym rozmiarze fizycznym i charakteryzujące się niskim poborem energii wynoszącym nie więcej niż 1200W
3	Dostępność	Macierz klasy Enterprise pracująca w trybie symetric Active-Active (nie ALUA) co oznacza iż w przypadku utylizacji na poziomie 100% zapewnia: - uzyskanie wysokiej dostępności na poziomie 99.9999% dla pojedynczej macierzy. - braku spadku wymaganej wydajności macierzy w przypadku awarii połowy kontrolerów - braku spadku wymaganej wydajności w przypadku awarii dwóch dysków z tej samej pooli RAID - 100% odczytu z pełnej pojemności

4	Niezawodność	Rozwiązanie musi oferować dostępność na poziomie minimum 99,9999% lub wyższym w obrębie pojedynczej macierzy. Potwierdzenie realizacji tej funkcjonalności musi znajdować się w oficjalnej dokumentacji producenta oferowanego sprzętu. Architektura rozwiązania nie może mieć pojedynczego punktu awarii (SPOF). Dane musza być dostępne w przypadkach: - awarii jednej linii zasilania, - awarii dowolnego kontrolera, - awarii dowolnych dwóch nośników danych użytkownika, - awarii dowolnego portu FC/iSCSI, - awarii dowolnego modułu pamięci RAM lub dowolnego procesora kontrolera. Awaria i niedostępność pojedynczego kontrolera macierzy nie może powodować spadku wydajności całego rozwiązania – brak efektu tzw. „Degraded Performance failover". Oznacza to iż macierz musi posiadać identyczną wydajność w obydwu stanach: awarii oraz barku awarii. Zmiana wersji oprogramowania zarządzającego rozwiązaniem lub oprogramowania wbudowanego w kontrolery rozwiązania nie może powodować utraty dostępu do danych. Rozwiązanie nie może zawierać komponentów zapasowych, które nie są wykorzystywane podczas pracy urządzenia (np. zapasowy kontroler, dysk hot spare). Oferowana macierz musi gwarantować optymalizację inwestycji poprzez ciągłe wykorzystanie wszystkich elementów dostarczanego sprzętu. Rozwiązanie musi umożliwiać wymianę na gorąco (bez zatrzymywania dostępu do danych) następujących komponentów: kontrolerów, zasilaczy, wentylatorów, portów front-end i back-end, nośników NVME. Rozwiązanie musi umożliwiać bezpieczne wyłączenie urządzenia niepowodujące utraty danych użytkownika. Dane przechowywane w pamięci urządzenia muszą zostać trwale zapisane na nośniki Flash przed całkowitym wyłączeniem macierzy na skutek awarii bądź interwencji manualnej.

5	Obsługa komunikacji do hosta	Rozwiązanie musi być zbudowane w oparciu o dwa lub wielokrotność dwóch kontrolerów macierzowych pracujących symetrycznie w trybie active-active w zakresie obsługi danych wejściowych i wyjściowych. Tryb active-active jest wymagany niezależnie od liczby kontrolerów w macierzy. Macierz z włączonym trybem active-active nie może ograniczać wymaganej wydajności, pojemności oraz funkcjonalności (np. ilości wspieranych snapshotów). Niedopuszczalne są rozwiązania dual-active oraz ALUA (Asymmetric Logical Unit Access). Ze względu na specyfikę protokołu NVMe wymagane jest, aby połączenia pomiędzy wszystkimi kontrolerami macierzowymi były realizowane poprzez magistrale PCIe, dla konfiguracji: - dwu-kontrolerowej - cztero-kontrolerowej (warunek ten musi być spełniony nawet w przypadku, gdy opcja ta występuje jako element rozbudowy).
6	Architektura dostępu do danych	Macierz musi korzystać z globalnej puli nośników i danych niezależnie od wykorzystywanego kontrolera. Niedopuszczalne jest rozwiązanie, w którym LUNy bądź urządzenia fizyczne typu dysk/moduł są przypisywane do kontrolera. Rozwiązanie musi wspierać pracę na wszystkich portach front-end w trybie round-robin z niezmiennymi czasami odpowiedzi, niezależnie od aktualnie wykorzystywanego portu, kontrolera i wolumenu. Niedopuszczalne jest rozwiązanie typu ALUA.
7	Wydajność	Minimalna wymagana wydajność rozwiązania musi być osiągalna z aktywnymi i pracującymi wszystkimi funkcjami redukcji danych, niezależnie od stopnia zapełnienia przestrzeni fizycznej danymi tj. od zajętości 1 do 100%. Jeżeli macierz w obrębie dwóch kontrolerów nie jest w stanie utrzymać 100% wydajności, wymagane jest dostarczenie konfiguracji cztero-kontrolerowej zapewniającej ww. wydajność Niezależnie od rodzaju zapisanych danych i przy macierzy zapełnionej w przynajmniej 70% fizycznej pojemności, roz-

		wiązanie w oferowanej konfiguracji musi oferować następującą wydajność na całej powierzchni dostępnej dla użytkownika, z aktywnymi i pracującymi wszelkimi oferowanymi funkcjami redukcji danych (thin-provisioning, deduplikacja, kompresja): - co najmniej 300 000 losowych operacji odczytu wykonywanych blokiem 16 kB ze średnim czasem odpowiedzi mierzonym po stronie hosta nieprzekraczającym 2 ms, - co najmniej 180 000 losowych operacji Zapisu wykonywanych blokiem 16 kB ze średnim czasem odpowiedzi mierzonym po stronie hosta nieprzekraczającym 2 ms, - co najmniej 230 000 losowych operacji odczytu/zapisu Read 50%/Write 50%wykonywanych blokiem 16 kB ze średnim czasem odpowiedzi mierzonym po stronie hosta nieprzekraczającym 2 ms, - odczyt danych na poziomie co najmniej 5.6 GiB/s, - zapis danych na poziomie co najmniej 2.8 GiB/s. Te same parametry wydajnościowe muszą być spełnione w przypadku, gdy w czasie testów trwających minimum 60 minut, na wolumenach poddanych obciążeniu: - tworzone są kopie migawkowe - dane są dodawane i usuwane - z macierzy tymczasowo usunięte zostają minimum dwa nośniki Flash. Zamawiający zastrzega sobie prawo do wykonania ww. testów wydajnościowych na etapie wdrożenia z wykorzystaniem oprogramowania Vdbench.
8	Skalowalność macierzy	Macierzy musi umożliwiać skalowalność wertykalną (scale-up) to jest taką gdzie konfiguracja inicjalna zaczyna się od niepełnego obsadzenia dyskami i pozwala na instalowanie kolejnych dysków w wolnych slotach półki oraz o dodatkowe półki bez wpływu na dostępność do danych, oraz bezprzerwową aktualizację do wyższego modelu macierzy.
9	Skalowalność kontrolerów	Rozbudowa macierzy musi być wykonywana na gorąco, bez konieczności migrowania danych na inne urządzenia i bezprzerwowo dla działania aplikacji korzystających z rozbudowywanej macierzy.

10	Bezprzerwowy upgrade kontrolerów	Oferowana macierz musi umożliwiać bezprzerwowe przejście do wyższego modelu macierzy tego samego producenta poprzez np. wymianę kontrolerów lub poprzez dołożenie dodatkowych kontrolerów, które będą tworzyły z oferowanymi w postępowaniu kontrolerami jeden spójny system macierzowy zarządzany z jednej konsoli administracyjnej. Wymiana kontrolerów lub ich dołożenie nie może powodować przerwy w dostępie do danych oraz utraty którejkolwiek z wymaganych funkcjonalności.
11	Skalowalność portów	Macierz musi posiadać (bez stosowania dodatkowych przełączników lub koncentratorów) możliwość skalowalności do minimum 20 portów Fibre Channel 32 Gbps lub 16 portów Ethernet 25 Gbps SFP28 w obrębie dwóch kontrolerów,
12	Pojemność	Oferowana macierz musi składać się z minimum 10 nośników Flash NVMe nie mniejszych niż 18 TiB (tebibytes) każdy oraz być rozbudowywalna do minimum 20 nośników flash. Macierz w oferowanej konfiguracji musi zapewniać minimum 140 TiB gwarantowanej przestrzeni użytkowej bez uwzględnienia wszelkich efektywności upakowania i redukcji danych. Macierz musi umożliwiać rozbudowę do co najmniej 330 TiB przestrzeni użytkowej w ramach pojedynczej obudowy. Zapełnienie macierzy w 100% dostępnej pojemności nie może powodować utraty dostępu do danych.
13	Kompatybilność z - (NVMe)	Macierz musi wykorzystywać protokół NVMe do wszystkich operacji wewnętrznych jak i komunikacji z dodatkowymi półkami dyskowymi niezależnie od skali oferowanego systemu. Niedopuszczalne jest stosowanie protokołów typu SAS bądź FC w żadnym wewnętrznym komponencie rozwiązania. Wykluczone jest tym samym stosowanie translacji kodowania NVMe do SAS pomiędzy różnymi komponentami macierzy. Macierz musi być wyposażona w procesory wyposażone we wsparcie dla protokołu NVME. Zamawiający dopuszcza architekturę X86 dwóch producentów procesorów Intel (z

		generacją co najmniej Skylake) oraz AMD (z generacją Epyc)
14	Bezpieczeństwo danych	Rozwiązanie musi szyfrować wszelkie przechowywane dane minimum algorytmem AES-256 lub silniejszym oraz szyfrować wszystkie nośniki flash obsługiwane w urządzeniu. Szyfrowanie danych nie może mieć wpływu na wydajność rozwiązania. Zgodnym z certyfikacją FIPS 140-2. Algorytm szyfrowania musi posiadać możliwość przechowywania klucza szyfrującego w: - Serwerze kluczy zgodnym ze standardem KMIP - kartach SmartCard podłaczonych poprzez czytniki do portów USB macierzy. - systemie macierzowym - wsparcie dla kluczy Yubikey Klucz szyfrujący musi być domyślnie przechowywany na macierzy i generowany w sposób uniemożliwiający odczyt danych z usuniętych z macierzy nośników Flash. Szyfrowanie musi być rozwiązaniem niezależnym od producenta modułów Flash w pełni kontrolowanym przez producenta macierzy.
15	Ochrona nośników danych	W celu zapewnienia ochrony danych każdy dysk oraz moduł w macierzy musi przechowywać w tym samym momencie dane parzystości, dane aplikacji oraz przestrzeń zapasową. Ochrona danych musi być realizowana za pomocą tzw. rozproszonej podwójnej parzystości na poziomie blokowym. Niedopuszczalne są klasyczne realizacje ochrony danych oparte grupy dysków w RAID 4/5/6 oraz RAID 10. W szczególności niedopuszczalne jest stosowanie dedykowanych dysków parzystości tzw. parity drives oraz dedykowanych dysków zapasowych tzw. hot spare drives. Niedopuszczalne jest stosowanie dysków dedykowanych tylko do konkretnych typów danych. Zaoferowane nośniki flash NVMe muszą wspierać, wszystkie typy RAID obsługiwane przez oferowany system macierzowy.

16		Rozwiązanie musi oferować mechanizm monitorowania trwałości nośników Flash i realizować funkcję proaktywnej odbudowy czyli zgłoszenia awarii nośnika jeszcze zanim jego komórki ulegną całkowitemu wypaleniu. Rozwiązanie musi oferować mechanizm weryfikacji odczytywanych danych, wykrywania i naprawiania uszkodzonych danych w sposób przezroczysty dla hosta. Rozwiązanie musi być odporne na jednoczesną awarię minimum dwóch dowolnych nośników Flash, niezależnie od skali i konfiguracji rozwiązania. W przypadku awarii dwóch nośników macierz musi zapewnić bezprzerwowy dostęp do wszystkich danych na macierzy.
17	Połączenia do hostów oraz replikacji - wymaganie globalne	Niedopuszczalne jest stosowanie sprzętu pośredniczącego oraz niedopuszczalne jest wykorzystywanie ww. portów FCP do komunikacji z hostami. Niedopuszczalne jest wykorzystywanie portów FC oraz SAS do łączenia kontrolerów macierzowych. Zastosowane karty FC muszą obsługiwać protokół NVMe-o-F (NVMe over Fabrics). Zmiana wykorzystywanego przez karty protokołu pomiędzy FC a NVMe-o-F musi być możliwa dla administratora oraz odbywać się bezprzerwowo z punktu widzenia dostępu do danych. Zabronione jest emulowanie protokołów blokowych takich jak FCP oraz iSCSI, macierz musi natywnie bez warstw pośredniczących wspierać powyższe protokoły.
18	Porty ETHERNET	Rozwiązanie musi posiadać natywne podłączenie do hostów poprzez protokoły NAS (CIFS/NFS) zapewniając minimalną ilość 4 portów 25 Gbit/s SFP28 Ethernet (min 2 per kontroler). Zmiana przepustowości portu 25Gbit/s na 10Gbit/s musi być możliwa poprzez wymianę modułu SFP+ a nie całej karty HBA w kontrolerze.
19	Porty FC (HBA)	Rozwiązanie musi posiadać natywne podłączenie do hostów poprzez protokół FCP zapewniając minimalną ilość 4 portów 32 Gbit/s SFP+ Ethernet (min 2 per kontroler). Niedopuszczalne jest stosowanie sprzętu pośredniczącego iSCSI-FC itp.

		Zmiana przepustowości portu 32Gbit/s na 64Gbit/s musi być możliwa poprzez wymianę modułu SFP+ a nie całej karty HBA w kontrolerze.
20	Porty do zarządzania	Każdy kontroler musi posiadać 2 porty RJ45 każdy 1Gbit/s Ethernet przeznaczone do zarządzania. System musi wspierać możliwość zarządzania portami dedykowanymi do replikacji lub ruchu iSCSI.
21	Funkcje redukcji i prezentacji danych	Rozwiązanie musi realizować funkcję thin-provisioningu dla wszystkich udostępnianych wolumenów oraz dostarczenie funkcji space reclamation tzn. rozwiązanie musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny i inicjowany bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych, ani na zewnętrznych systemach. Rozwiązanie musi zapewniać mechanizm kompresji danych w trybie in-line. Kompresja musi być integralną częścią systemu macierzowego i nie może być w żaden sposób możliwa do wyłączenia przez administratora macierzy lub serwis producenta. Rozwiązanie musi zapewniać mechanizm deduplikacja danych w trybie in-line. Deduplikacja nie może być w żaden sposób zatrzymywana ani możliwa do wyłączenia przez administratora macierzy. Deduplikacja danych musi być realizowana na bloku o rozmiarze maksimum 4KB. Dla każdego wolumenu macierzy musi zachodzić jednocześnie kompresja i deduplikacja danych. Niedopuszczalne jest stosowanie tych funkcjonalności zamiennie lub rozłącznie. Baza deduplikowanych bloków musi być globalna, tj. musi obejmować bloki danych zapisanych na wszystkich wolumenach i nośnikach w macierzy, zarządzanych przez wszystkie kontrolery macierzy, niezależnie od skali rozwiązania, ilości wolumenów oraz typu danych przechowywanych na wolumenach i pulach nośników.

		Rozwiązanie musi prezentować aktualny całkowity współczynnik redukcji danych oraz niezależnie uzysk realizowany poprzez thin-provisioning, globalną deduplikację i kompresję.
22	Wbudowane funkcje macierzy	Rozwiązanie musi oferować funkcję tworzenia natychmiastowych kopii wolumenów oraz oferować możliwość utworzenia przynajmniej 40000 kopii wolumenu. Rozwiązanie musi zapewniać hierarchiczne tworzenie kopii (np. kopia z kopii z kopii). W momencie utworzeni kopia nie może zajmować dodatkowej przestrzeni dyskowej dostępnej dla użytkownika. Nie dopuszcza się rozwiązań, które realizują powyższą funkcjonalność na zasadzie „Kopiowania przy zapisie” (Copy-on-write) Rozwiązanie musi oferować możliwość natychmiastowego odtworzenia wolumenu z dowolnej kopii utworzonej z tego wolumenu bądź znajdującej się w dowolnym miejscu hierarchii kopii tego wolumenu. Odtworzony wolumen musi być natychmiast dostępny dla hosta w trybie read/write. Rozwiązanie musi oferować możliwość natychmiastowego odświeżenia dowolnej kopii z dowolnej innej kopii lub wolumenu w ramach jego hierarchii. Odtworzona kopia musi być natychmiast dostępna dla hosta w trybie read/write. Rozwiązanie musi umożliwiać tworzenie grup spójności, które gwarantują spójne kopiowanie, odtwarzanie i odświeżanie grupy wolumenów. Dane zawarte we wszystkich kopiach muszą być objęte globalną - tj. obejmującą wszystkie nośniki w całej macierzy - deduplikacją i kompresją danych. System operacyjny macierzy musi umożliwiać tworzenie spójnych kopii całych baz danych bądź aplikacji bez wykorzystania dodatkowego, zewnętrznego oprogramowania. Musi istnieć możliwość utworzenia wielu kopii naraz bez wykorzystania dodatkowej przestrzeni na macierzy.
23	Replikacja	Rozwiązanie musi posiadać funkcjonalność replikacji synchronicznej umożliwiające utworzenie z obu macierzy kla-

		stra active-active (pomiędzy dwiema serwerowniami zlokalizowanymi w osobnych budynkach) oraz zapewniać wszystkie komponenty sprzętowe niezbędne do realizacji funkcjonalności replikacji. Jeżeli takowe komponenty są używane ich właściwości - typu rozmiar fizyczny - muszą zostać wliczone w całkowity rozmiar rozwiązania. Replikacja synchroniczna musi być możliwa dla minimum jednego wolumenu (LUNa) oraz jednocześnie dla wielu wolumenów (LUNów), a zmiana ilości replikowanych wolumenów nie może wymagać zmiany konfiguracji sprzętowej macierzy. Replikacja musi być możliwa do realizacji poprzez protokół FC oraz IP. Utworzony w ten sposób klaster udostępnia ten sam wolumen do odczytu/zapisu na obu zaoferowanych macierzach. Zawartość wolumenów klastra musi być identyczna na obu systemach w każdym momencie realizowania klastra. Rozwiązanie replikacji synchronicznej musi bazować na domyślnych sterownikach MPIO systemów operacyjnych bez konieczności dogrywania dodatkowych sterowników.
24	Replikacja kaskadowa	Rozwiązanie musi umożliwiać kaskadową replikacje asynchroniczną – oznacza to iż każdy wolumen replikujący się synchronicznie do drugiej lokalizacji może być replikowany z lokalizacji drugiej do lokalizacji trzeciej w sposób asynchroniczny.
25	Replikacja JurnalLog	Funkcjonalność replikacji bazującej na JournalLog może być dostarczona zarówno jako mechanizm wbudowany jak również dodatkowa aplikacja zewnętrzna ze wszystkimi wymaganymi komponentami sprzętowymi oraz licencyjnymi. Replikacja powinnaumożliwiać: - testowanie operacji Failover - komunikacje poprzez FC oraz Eth - ustawienie niezależnych schematów kopii migawkowych na macierzach biorących udział w replikacji
26	Ochrona wolumenów przed atakiem ransomware	Oferowany system powinien zapewniać ochronę wolumenów przeciw atakom Ransomware. Dane na wolumenach muszą być albo zabezpieczone przed skasowaniem/nadpisaniem przez nieautoryzowaną operację, albo musi być

		możliwe natychmiastowe odtworzenie danych z kopii migawkowej zabezpieczonej przed usunięciem na okres minimum 1 miesiąca. Ochrona musi zapewniać mechanizmy uodparniające system macierzowy przed: - niepowołanym skasowaniem snapshotów nawet przez użytkownika zalogowanego jako administrator macierzy - umożliwiać integrację z replikacją macierzową - zmianą retencji danych - zmianą czasu/serwera czasu – uniezależnienie macierzy oraz snapshotów od serwera czasu - niepowołaną autoryzacją kasowania danych - wspierać zarówno dostęp plikowy jak i blokowy.
27	Dostęp Plikowy	System musi wspierać : CIFS w wersjach 2.0, 2.1, 3.0.2, 3.1.1 oraz NFS v3 lub równoważny
28	Monitoring	W ramach dostawy systemu macierzowego wymagane jest dostarczenie platformy analityczno-raportującej w postaci portalu dostępnego przez przeglądarkę WWW. Platforma powinna zbierać w sposób automatyczny logi z macierzy oraz prezentować je w postaci grafów i raportów, wymagane są następujące funkcjonalności ww. platformy: a. Wyświetlanie używanej przestrzeni wraz ze wskaźnikiem redukcji danych opartych o algorytmy deduplikacji oraz kompresji bez ThinProvisioningu; globalnie dla macierzy oraz lokalnie dla wolumenu b. Portal musi umożliwiać predykcję przyrostu przestrzeni wraz z analizą przyszłej rozbudowy. c. Wyświetlanie historii wydajności poszczególnych zasobów z uwzględnieniem parametrów: latencji, Read&Write IOps, oraz przepustowości; globalnie dla macierzy oraz lokalnie dla wolumenu d. Możliwość tworzenia raportów z pojemności, wydajności, predykcji przyszłej przestrzeni, logów autoryzacji do urządzenia, poziomu oraz czasu wsparcia technicznego. e. Wyświetlanie statusu wykonanych operacji jak Snapshoty, Replikacja synchroniczna f. Wyświetlanie ostrzeżeń o zagrożeniach informacji o logujących się użytkownikach oraz wykonanych komendach na macierzy.

		g. Wyświetlanie informacji na temat otwartych oraz zamkniętych spraw serwisowych h. Portal musi umożliwiać symulację przyrostu pojemności w zależności od rodzaju aplikacji i. Algorytm weryfikacji poprawnej konfiguracji oraz możliwości upgradu oprogramowania macierzowego. j. Umożliwiać automatyczny upgrade macierzy h. Wyświetlanie poboru systemu wraz wskazówkami optymalizacji.
29	Zarządzanie	Rozwiązanie musi udostępniać graficzną konsolę zarządzającą (GUI) poprzez interfejs Web (HTML5), która umożliwia monitorowanie stanu i obciążenia macierzy. Konsola graficzna jest dostępna poprzez przeglądarkę internetową i jest elementem systemu operacyjnego macierzy. Monitorowanie urządzenia musi być dostępne z panelu GUI administratora macierzy i musi obejmować swoim zakresem dane historyczne z okresu przynajmniej 1 roku wstecz. Rozwiązanie musi umożliwiać monitorowanie: - wykorzystania całkowitej pojemności fizycznej, - wykorzystania pojemności logicznej, - globalnego współczynnika redukcji danych, - wartości transferu danych (w MB/s) oraz ilości operacji (IOPS) Rozwiązanie musi być zarządzane poprzez linię komend (CLI) dostępną poprzez protokół SSH. Dostęp do linii komend poprzez SSH musi być możliwy bez podawania hasła tj. przy wykorzystaniu kluczy uwierzytelniających. Rozwiązanie musi udostępniać interfejs REST API oraz SNMP do komunikacji z zewnętrznymi narzędziami monitorującymi. Macierz musi mieć wbudowane procedury pełnej i automatycznej diagnostyki elementów oraz możliwość natychmiastowego raportowania błędów do administratorów oraz do centrum wsparcia technicznego producenta w trybie 24/7/365.
30	Licencja	Rozwiązanie musi być dostarczone z licencjami na wszystkie dostępne dla systemu funkcjonalności oraz dyski dla

		maksymalnej do uzyskania w oferowanym modelu pojemności RAW.

3.3. Wymagania funkcjonalne dla Oprogramowania Dedykowanego systemu SZIRS

3.3.1. Opis Systemu

System ma centralizować dane o rezerwach strategicznych pochodzące z różnych systemów zarządzania rezerwami, w szczególności z systemów magazynowych lub o specyfice zbliżonej do systemów magazynowych.

3.3.2. Podsystem Centralizacji Danych

System ma spójnie zarządzać informacją o rezerwach, pochodzącą z wielu źródeł zróżnicowanych co do nazewnictwa, struktury informacji i w szczególności budowy indeksów materiałowych, z uwzględnieniem:

1) wskazania indeksu materiałowego i pozycji w tym indeksie, opisującej materiał będący rezerwą
2) wszelkich opisów i dokumentacji opisujących rodzaj lub charakter materiału będącego pozycją rezerwy
3) informacji teleadresowej o umiejscowieniu materiału
4) informacji kontaktowej o osobie lub osobach fizycznych i prawnych utrzymujących rezerwę
5) umiejscowienia geograficznego i terytorialnego materiału
6) instrukcjach, obowiązujących procedurach dostępu i planach budynków, magazynów ułatwiających dostęp do lub odnalezienie materiału (np. w przypadku magazynu wysokiego składowania aleja, regał, nr półki)
7) informacji ilościowej o materiale wyrażonej w przeznaczonych do tego słownikowych jednostkach miary (tony, litry, sztuki)
8) informacje o sposobie zapakowania materiału (np. standardowa paleta = 1000 sztuk)
9) informacje o sposobie porcjowania materiału i występujących w nim substancji aktywnych (np. farmaceutyki – środki przeciwgorączkowe, liczba miligramów paracetamolu na jednostkę leku)
10) informacje o masie brutto, netto i tara pakunków
11) informacje o gabarycie pakunków
12) opis jednostek materiału z dokładnością do sztuki (numer seryjny) lub partii wg producenta (np. farmaceutyki, żywność konserwowa)

13) terminy: przydatności do użycia, produkcji, kontroli na miejscu, planowanej kontroli na miejscu
14) opis sposobu zakonserwowania i sposobu rozkonserwowania materiału
15) informacja ilościowa faktyczna i planowana
16) informacja o stanie jakościowym materiału (np. skażone, obniżona skuteczność)
17) wartość materialna rezerwy
18) wartość inna (wg arbitralnych skal) rezerwy
19) Wdrożenie w ramach Umowy obejmuje migrację danych z jednego systemu magazynowego.

3.3.3. Podsystem Wyszukiwania i Sprawozdawczości

System ma umożliwiać dynamiczne raportowanie informacji o rezerwach, w tym spójne i skuteczne wyszukiwanie informacji o rezerwach pochodzących z różnych systemów zarządzania tymi informacjami tj. w różnym formacie i sposobie zapisu tych informacji. Mechanizmy wyszukiwania i raportowania informacji muszą wykazywać dużą tolerancję na jakość danych tj. na zjawiska takie jak niejednoznaczność danych słownikowych pochodzących z różnych źródeł, różnorodność konstrukcji indeksów materiałowych pochodzących z różnych systemów zarządzania informacjami o rezerwach. Mechanizm wyszukiwania i raportowania powinien umożliwiać filtrowanie danych wg wszystkich cech jakie mogą być przypisane rezerwie lub dotyczącej jej pozycji indeksu materiałowego. Szczególnie istotne jest uwzględnienie aspektów terytorialnych dyslokacji rezerw tj.

1) możliwość wskazania gmin, powiatów, województw bądź inaczej wskazanych regionów i innych obszarów dla których przeprowadzone zostanie wyszukiwanie lub raportowanie

3.3.4. Podsystem Wymiany Danych

System ma zawierać mechanizm wsadowego, nadzorowanego i rozliczalnego aktualizowania informacji o rezerwach z systemów zewnętrznych i do systemów zewnętrznych umożliwiający wykonanie synchronizacji w warunkach całkowitego technicznego odseparowania tych systemów.

4. Organizacyjny Opis Przedmiotu Zamówienia

4.1. Terminy Realizacji Przedmiotu Zamówienia

1. Wykonawca zobowiązany jest do wykonania przedmiotu zamówienia określonego w Rozdziale 3 w terminach wskazanych w Umowie:

1) Faza 1 - dostawa Sprzętu i Obramowania Standardowego, obejmująca serwery, macierze dyskowe, przełączniki SAN, przełączniki LAN, platformę zarządzania kontenerami oraz system backupu wraz z zapewnieniem gwarancji oraz usług serwisowych.
2) Faza 2 - instalacja, i konfiguracja sprzętu i oprogramowania wymienionego w ppkt. 1,
3) Faza 3 - wdrożenie systemu zarządzania informacją o rezerwach strategicznych do dnia.

4.2. Wymagania w zakresie gwarancji

4.2.1. Wymagania ogólne

1. Wykonawca udziela Zamawiającemu Gwarancji na warunkach opisanych w niniejszym rozdziale na:
   1.1. Sprzęt,
   1.2. Oprogramowanie Standardowe,
   1.3. Oprogramowanie Dedykowane
   1.4. Pozostałe Produkty powstałe w wyniku realizacji Umowy.
2. Wykonawca zapewnia, że Sprzęt i Oprogramowanie Standardowe przez niego dostarczone objęte jest gwarancją producentów, która obowiązuje przez 36 miesięcy od daty odbioru ilościowego Sprzętu. Wady Sprzętu i Oprogramowania Standardowego będą usuwane zgodnie z wymaganiami opisanymi w niniejszym rozdziale.
3. Okres udzielanej Gwarancji liczony jest dla:
   3.1. Sprzętu – od daty podpisania protokołu Ilościowego,
   3.2. Oprogramowania Standardowego– od daty podpisania protokołu Ilościowego,
   3.3. Oprogramowania Dedykowanego– od daty podpisania protokołu testów systemu,
   3.4. dla innych Produktów – od daty Odebrania przez Zamawiającego danego Produktu.
4. Zakres świadczeń w ramach Gwarancji obejmuje:
   4.1. usuwanie Wad Sprzętu i Oprogramowania zgodnie z Czasami Reakcji, Czasami Naprawy, Czasami Obejścia i Maksymalnymi dozwolonymi czasami funkcjonowania Obejścia dla poszczególnych kategorii Wad,
   4.2. dostarczanie, instalację i konfigurację nowych wersji Oprogramowania,
   4.3. dostarczanie, instalację i konfigurację aktualizacji Oprogramowania,
   4.4. prowadzenie wszelkich działań prewencyjnych mających na celu wydłużenie czasu bezawaryjnej pracy Infrastruktury Teleinformatycznej,
5. Wykonawca zobowiązuje się do świadczenia usług w ramach Gwarancji w sposób zapobiegający utracie jakichkolwiek danych przetwarzanych z wykorzystaniem wdrożonych komponentów sprzętowych i oprogramowania.
6. W ramach świadczenia przez Wykonawcę usług w ramach Gwarancji, Wykonawca zobowiązany jest do umożliwienia osobom wskazanym przez Zamawiającego obserwacji prac Wykonawcy.

7. W przypadku wykrycia przez Zamawiającego Wady, Zamawiający dokona kwalifikacji zgłoszenia (Błąd Krytyczny / Błąd Poważny / Błąd Drobny/Zapytania) według własnego uznania na podstawie zdefiniowanych kryteriów. Zgłoszenie zawierać będzie posiadane przez Zamawiającego informacje na temat nieprawidłowego działania Infrastruktury Teleinformatycznej, istotne w ocenie Zamawiającego dla zdiagnozowania i usunięcia nieprawidłowości w działaniu Infrastruktury Teleinformatycznej.
8. Wykonawca w ramach przygotowania Dokumentacji musi przygotować i przedstawić Zamawiającemu do akceptacji plan obsługi serwisowej zawierającą szczegółowe informacje na temat realizacji zgłoszeń, doboru kryteriów w konkretnych przypadkach awaryjnych oraz ścieżki ich obsługi.
9. Formalne potwierdzenie Zgłoszenia stanowi przesłany przez Zamawiającego do Wykonawcy Protokół Zgłoszenia Wady.
10. Wykonawca zobowiązuje się rejestrować zgłaszane Wady wykorzystując rozwiązania umożliwiające raportowanie Zgłoszeń - w tym Czas Reakcji, Czas Obejścia oraz Czas Naprawy, Maksymalny dozwolony czas funkcjonowania Obejścia.
11. Wykonawca będzie przyjmował Zgłoszenia przez cały czas, tj. w systemie 24/7/365.
12. W razie otrzymania przez Wykonawcę Zgłoszenia lub w razie uzyskania przez Wykonawcę wiedzy o wystąpieniu Wady z innego źródła niż Zgłoszenie Wykonawca zobowiązany będzie do podjęcia działań zmierzających do usunięcia Wady.
13. Jeżeli Zamawiający nie wie o istnieniu Wady, Wykonawca poinformuje niezwłocznie Zamawiającego o jej wystąpieniu.
14. Jeżeli Wada została wykryta przez Wykonawcę, Wykonawca nada jej odpowiednią wstępną kategorię (Błąd Krytyczny / Błąd Poważny / Błąd Drobny/Zapytania). Po niezwłocznym powiadomieniu przez Wykonawcę Zamawiający ma prawo zmienić kategorię błędu.
15. Wykonawca zobowiązany jest do potwierdzenia przyjęcia Zgłoszenia odpowiednim wpisem we własnej aplikacji serwisowej (dotyczy to również Zgłoszeń składanych pocztą elektroniczną lub faksem). Chwila potwierdzenia przyjęcia Zgłoszenia nie ma wpływu na Czas Reakcji, Czas Obejścia, Czas Naprawy i Maksymalny dozwolony czas funkcjonowania Obejścia. Wykonawca jest zobowiązany do udostępnienia Zamawiającemu własnej aplikacji serwisowej w zakresie przeglądania Zgłoszeń związanych z realizacją Umowy.
16. Jeżeli Wykonawca stwierdzi, iż nieprawidłowe działanie SZIRS, którego dotyczy Zgłoszenie nie jest spowodowane Wadą, za którą odpowiedzialny jest Wykonawca, wówczas Wykonawca zobowiązany jest:
    16.1. wskazać przyczynę nieprawidłowego działania SZIRS poprzez wskazanie elementu, który ją powoduje,
    16.2. udzielić wsparcia Zamawiającemu lub innej osobie trzeciej wskazanej przez Zamawiającego usuwającej przyczyny Zgłoszenia, w tym udzielić takiej osobie wszelkich informacji

o dostarczonej infrastrukturze teleinformatycznej potrzebnych do przywrócenia pełnej funkcjonalności SZIRS.

17. Jeżeli Wykonawca stwierdzi, iż nieprawidłowe działanie Infrastruktury Teleinformatycznej spowodowane jest wadliwym działaniem Sprzętu, którego Wykonawca nie jest w stanie usunąć, wówczas Wykonawca zobowiązany jest w Czasie Naprawy dostarczyć inny sprzęt realizujący funkcje wadliwego Sprzętu o parametrach nie gorszych niż urządzenia wadliwe.
18. Po przeprowadzeniu Naprawy, Wykonawca zgłosi ją do odbioru poprzez wypełnienie w dwóch egzemplarzach Protokołu z Naprawy, a Zamawiający przystąpi niezwłocznie do weryfikacji dokonanej Naprawy.
19. Po weryfikacji dokonania Naprawy Zamawiający niezwłocznie potwierdzi na Protokole z Naprawy skuteczność lub nieskuteczność Naprawy. Data i godzina podpisania ww. dokumentu przez przedstawiciela Zamawiającego jest datą i godziną wykonania usługi Naprawy.
20. W przypadku stwierdzenia dokonania skutecznej Naprawy Wykonawca zamyka Zgłoszenie i potwierdza jego wykonanie poprzez „zamknięcie" zgłoszenia w aplikacji serwisowej.
21. Naprawa, co do której Wykonawca poinformował o jej wykonaniu, a która została odrzucona przez Zamawiającego ze względu na fakt, iż testy przeprowadzone przez Zamawiającego wykazują, że Wada nadal występuje, trwa do czasu jej skutecznego wykonania.
22. Wykonawca zobowiązany jest do prowadzenia ewidencji otwartych i zamkniętych Zgłoszeń, obejmującej w szczególności opis stanu realizacji danej Naprawy. Powyższe dane dostępne są cały czas dla Zamawiającego za pośrednictwem aplikacji serwisowej.
23. Wraz z dokonaniem Naprawy Wykonawca zobowiązany jest opracować i przekazać Zamawiającemu odpowiednią Dokumentację, o ile zachodzi taka potrzeba.
24. Jeżeli Wykonawca nie dokona Naprawy Wady w terminie określonym w niniejszym załączniku to Zamawiający może:
    24.1. zawiadamiając uprzednio Wykonawcę usunąć Wadę we własnym zakresie lub powierzyć jej usunięcie innym podmiotom trzecim na ryzyko i koszt Wykonawcy, co nie spowoduje utraty przysługujących Zamawiającemu uprawnień z tytułu Gwarancji– przy czym koszty poniesione przez Zamawiającego przy usunięciu Wady mogą być potrącone z wynagrodzenia przysługującego Wykonawcy lub z zabezpieczenia należytego wykonania przedmiotu Umowy, na co Wykonawca wyraża zgodę;
    24.2. obciążyć Wykonawcę karą umowną.
25. Każdy miesiąc świadczenia usług w ramach Gwarancji będzie potwierdzany przez Wykonawcę odpowiednim raportem. Raport zostanie przygotowany Wykonawcę w ciągu 5 Dni Roboczych po zakończeniu danego miesiąca i będzie określał liczbę zgłoszonych Wad wraz z opisem dotrzymania lub opóźnienia względem terminów wskazanych w rozdziale Poziomy SLA.
26. Jeżeli w trakcie realizacji zobowiązań z tytułu Gwarancji dojdzie do wprowadzenia zmian w Produktach, w szczególności w programach komputerowych, wówczas do przejścia autorskich

praw majątkowych do zmienionych Produktów lub Dokumentacji, w zakresie Produktów lub Dokumentacji będących wynikiem zmian. Przejście autorskich praw majątkowych do zmienionych programów komputerowych następuje z chwilą wykonania przez Wykonawcę zobowiązań w zakresie Gwarancji. W zakresie Oprogramowania, ich producent bądź Wykonawca z chwilą wykonania zobowiązań z tytułu Gwarancji udziela licencji. W przypadku, gdy przekazane kody źródłowe lub Dokumentacja zostaną zmodyfikowane zgodnie ze zdaniem poprzednim, Wykonawca przekaże Zamawiającemu niezwłocznie zmodyfikowane kody źródłowe oraz Dokumentację.

27. W momencie startu okresu Gwarancji Wykonawca zapewni dostępność dedykowanego Koordynatora Kontraktu Serwisowego, którego obowiązkiem będzie świadczenie usług prewencyjnych i optymalizacyjnych oraz koordynacja wszystkich prac serwisowych świadczonych na rzecz Zamawiającego w ramach niniejszej Umowy. Do momentu włączenia Koordynatora Kontraktu Serwisowego, rolę tę będzie pełnił, Kierownik Kontraktu.
28. W uzasadnionych przypadkach Strony mogą podjąć decyzję o wydłużeniu Czasu Naprawy.

4.2.2. Warunki Gwarancji Sprzętu

1. Gwarancją objęta jest całość dostarczonego Sprzętu.
2. Koordynator Kontraktu Serwisowego w przypadku Sprzętu:
   2.1. opracowuje i uzgadnia z Zamawiającym plan obsługi serwisowej (raz w roku),
   2.2. dwukrotnie w ciągu każdego roku trwania Umowy Koordynator Kontraktu Serwisowego opracowuje plan uaktualnienia oprogramowania wbudowanego dla Sprzętu - uaktualnienia te rozwiązują potencjalne problemy, zwiększają możliwości funkcjonalne lub zwiększają wydajność. Wykonawca udostępnia, planuje i zapewnia instalację uaktualnień w sposób minimalizujący zakłócenia w działalności Zamawiającego, Uaktualnienia nie mogą powodować braku dostępności systemów teleinformatycznych.
   2.3. raz w roku wykonuje kontrolę warunków pracy Sprzętu,
   2.4. raz w roku dostarcza ocenę techniczną poziomu dostępności pamięci masowej,
   2.5. informuje o najlepszych praktykach i zasadach postępowania.
3. Obsługa serwisowa będzie świadczona w języku polskim.
4. Wykonawca zapewni dostęp do serwisu elektronicznego producenta, który obejmuje możliwość pobrania aktualizacji i najnowszych wersji oprogramowania układowego (Firmware).
5. Dyski twarde muszą być naprawiane jedynie w miejscu użytkowania, a w przypadku konieczności wymiany uszkodzonych dysków twardych lub wymiany Sprzętu na wolny od wad, dyski twarde nie podlegają zwrotowi do Wykonawcy. Dodatkowo, jeżeli zostanie dostarczony sprzęt zastępczy na czas naprawy Sprzętu Zamawiającego, wyposażony w dyski twarde, po wykonaniu naprawy Sprzętu Zamawiającego, dyski twarde nie podlegają zwrotowi. W przypadku konieczności dokonania naprawy Sprzętu wyposażonego w dyski twarde poza miejscem użytkowania, dyski twarde pozostają u Użytkownika.

6. Przedstawione przez Wykonawcę i producenta Sprzętu warunki serwisu nie mogą wprowadzać obostrzeń względem Zamawiającego w zakresie samodzielnej rekonfiguracji Sprzętu i oprogramowania poprzez jakiekolwiek ograniczenie lub utratę zamówionych świadczeń serwisowych. W szczególności dotyczy to:
   6.1. Instalacji, rekonfiguracji i aktualizacji oprogramowania systemowego, narzędziowego i aplikacyjnego,
   6.2. Instalacji poprawek dla oprogramowania systemowego, narzędziowego i aplikacyjnego,
   6.3. Instalacji i aktualizacji sterowników do zainstalowanych urządzeń lub podzespołów,
   6.4. Instalacji i konfiguracji podzespołów oraz urządzeń dodatkowych, np: kart rozszerzeń, modułów usługowych, urządzeń zewnętrznych, itp., wspieranych przez przedstawiciela bądź producenta sprzętu,
   6.5. Wykonywania czynności administracyjnych związanych z rekonfiguracją urządzeń np.: przełożeniem modułu lub podzespołu w obrębie lub pomiędzy urządzeniami, uaktualnianiem oprogramowania układowego (tzw. firmware), itp.
7. Parametry SLA określone są w rozdziale Poziomy SLA.

4.2.3. Warunki Gwarancji dla Oprogramowania Standardowego

1. Gwarancją objęta jest całość dostarczonego Oprogramowania Standardowego**,**
2. Wykonawca zapewni elektroniczny dostęp do informacji na temat posiadanego Oprogramowania Standardowego oraz biuletynów technicznych, poprawek, aktualizacji nowych wersji Oprogramowania Standardowego na stronach internetowych producentów tego oprogramowania.
3. Koordynator Kontraktu Serwisowego w przypadku Oprogramowania Standardowego:
   3.1. opracowuje i uzgadnia z Zamawiającym plan obsługi serwisowej (raz w roku),
   3.2. Wykonawca zapewnia Zamawiającemu dostęp do stron internetowych producentów, na których musza znajdować się aktualizacje, nowe wersje oraz zmiany w Oprogramowaniu opracowane przez producentów podczas trwania serwisu gwarancyjnego. Wykonawca zapewnia, że aktualizacje, nowe wersje lub zmiany są produktami wykonanymi przez producenta, a tym samym nie naruszają praw własności intelektualnej oraz że Wykonawca posiada prawo do ich dostarczania osobom trzecim na zasadach określonych w niniejszym załączniku
   3.3. Aktualizację oprogramowania układowego Sprzętu i Oprogramowania Standardowego, w szczególności dostarczania i instalacji nowych wersji oprogramowania układowego Sprzętu i Oprogramowania, dostarczania i instalacji wersji podwyższonych, wydań uzupełniających oraz poprawek programistycznych, bez dodatkowych opłat licencyjnych;
   3.4. Zapewnia możliwość zgłaszania błędów dotyczących Oprogramowania Standardowego bezpośrednio do producentów (producent musi być w tym przypadku pierwszą linią wsparcia) drogą elektroniczną przez portal producenta.

3.5. W ciągu każdego roku trwania Umowy Koordynator Kontraktu Serwisowego opracowuje plan aktualizacji Oprogramowania Standardowego,

3.6. informuje o najlepszych praktykach i zasadach postępowania.

4. Parametry SLA określone są w rozdziale Poziomy SLA.

4.2.4. Poziomy SLA

1. Wykonawca w ramach Gwarancji zobowiązuje się do zapewnienia w okresie świadczenia tych Usług wymaganych minimalnych Parametrów Dostępności funkcjonalności Systemu, odpowiednio w wysokości co najmniej **95**% dla Systemu. Przez Parametr Dostępności należy rozumieć czas dostępności Systemu oblicza się w ten sposób, że od sumy wszystkich godzin we wszystkie dni dla danego miesiąca kalendarzowego odejmuje się czas trwania planowanych okien serwisowych.
2. Parametr Dostępności w zakresie Dostępności określa się zgodnie z wzorem:

PD= (1 – (CA/CD))* 100%	PD – Parametr Dostępności CA – łączny czas niedostępności Systemu CD – łączny czas dostępności Systemu liczony jako iloczyn liczby dni w danym miesiącu oraz liczby 24

3. Poziomy SLA dla Sprzętu oraz Oprogramowania Standardowego oraz Oprogramowania Dedykowanego

Kategoria błędu	**Czas Reakcji**	**Czas Naprawy**	**Czas Obejścia**	**Maksymalny dozwolony czas funkcjonowania Obejścia**
Błąd Krytyczny	1 godzina	12 godzin	8 godzin	7 dni
Błąd Poważny	8 godzin	24 godziny	21 godzin	21 dni
Błąd Drobny	1 dzień	7 dni	5 dni	42 dni

Kategorie Błędów:

Błąd Krytyczny – Zdarzenie wpływające na działanie całego SZIRS, w sposób uniemożliwiający korzystanie z jego funkcjonalności. Zgłoszenie krytyczne dotyczy w szczególności sytuacji:

- awarii komponentu Sprzętowego lub Oprogramowania Standardowego powodującego brak dostępności do oglądu kamer oraz odtwarzania nagrań dla wszystkich użytkowników,
- awarii komponentu Sprzętowego lub Oprogramowania Standardowego prowadzącego do zawieszania lub powodowania opóźnienia w dostępie do SZIRS dla wszystkich użytkowników.

Błąd Poważny - Zdarzenie wpływające na działanie SZIRS, w sposób uniemożliwiający korzystanie z części funkcjonalności. Zgłoszenie poważne dotyczy w szczególności sytuacji:

- awarii komponentu Sprzętowego lub Oprogramowania Standardowego powodującego brak dostępności do części funkcjonalności SZRS dla dużej liczby użytkowników,
- zmniejszonej wydajności utrudniającej pracę użytkownikom.

Błąd Drobny - Zdarzenie wpływające na działanie systemu SZIRS w sposób uniemożliwiający korzystanie z części systemu lub jego funkcjonalności. Zgłoszenie drobne dotyczy w szczególności sytuacji:
- awarii komponentu Sprzętowego lub Oprogramowania Standardowego powodującego brak dostępności części SZIRS dla niewielkiej liczby użytkowników,
- zmniejszonej wydajności utrudniającej pracę niewielkiej liczbie użytkowników.

Zapytania - Zapytanie dotyczące problemu z obsługą Sprzętu lub Oprogramowania nie mający wpływu na dostępność funkcjonalności, charakteryzujący się następującymi cechami:
- zapytania dotyczące obsługi Sprzętu lub Oprogramowania Standardowego
- wyjaśnienia dotyczące dokumentacji
- zapytania dotyczące usprawnienia działania Sprzętu lub Oprogramowania Standardowego.

4.3. Wymagania w zakresie dokumentacji projektowej

4.3.1. Wstęp

Poniższy rozdział opisuje wymagania dotyczące dokumentacji projektowej, powykonawczej oraz eksploatacyjnej dla dostarczonego Sprzętu i Oprogramowania. W ramach realizacji wykonawca zobowiązany jest do opracowania następujących dokumentów:

1. Projekt Wykonawczy Wdrożenia dostarczanych elementów SZIRS,
2. Dokumentację Testową składającą się z:
    a. Planu Testów Akceptacyjnych,
    b. Scenariuszy Testów Akceptacyjnych.
3. Dokumentacja Powykonawcza, która powstanie jako uaktualnienie Projektu Wykonawczego SZIRS,
4. Procedury operacyjne,
5. Procedury Administracyjne,

4.3.2. Projekt Wykonawczy wdrożenia dostarczanych elementów SZIRS

Streszczenie

Dokument opisuje standard dokumentacji projektowej dla dostarczonego sprzętu i programowania oraz jego konfigurację i integrację z infrastrukturą Zamawiającego.

Opis

Cechy ogólne

- Dokumentacja musi być przygotowana zgodnie z szablonem ustalonym dla całej organizacji lub wyodrębnionego projektu.
- Kolejne sekcje dokumentacji muszą być numerowane w sposób kontekstowy – numeracja

Strona tytułowa

- Musi zawierać co najmniej następujące informacje:
    - Tytuł dokumentu
    - Nazwę lub numer tematu (zagadnienia)
    - Nazwę projektu
    - Informacje o autorach dokumentu:
        - Imiona, Nazwiska
        - Zajmowane stanowiska lub role pełnione w projekcie
        - Nazwa organizacji
- Strona tytułowa może zawierać inne, dodatkowe informacje, zgodnie z ustalonym szablonem, np.:
    - Identyfikator projektu, identyfikator dokumentu w projekcie lub inne identyfikatory,
    - Dodatkowe informacje precyzujące temat zagadnienia, np. nazwę podprojektu, określenie konkretnego tematu lub zagadnienia
    - Nazwę organizacji, nazwę jednostki organizacyjnej
    - Adres organizacji lub jednostki organizacyjnej
    - Bardziej szczegółowe informacje o autorach dokumentu:
        - Telefony kontaktowe
        - Adresy poczty elektronicznej

Metryka

- Metryka dokumentu musi zawierać co najmniej następujące informacje:
    - Określenie aktualnej wersji dokumentu
    - Datę publikacji dokumentu
    - Bardziej szczegółowe informacje o autorach dokumentu (jeśli nie były określone na stronie tytułowej):
        - Telefony kontaktowe
        - Adresy poczty elektronicznej
    - Historię zmian w dokumencie, zawierającą co najmniej następujące pola:
        - Wersję
        - Datę
        - Imiona i nazwiska autorów zmian
        - Krótki opis dokonanych zmian
    - Informację o akceptacji dokumentu – miejsca na podpisy właściwych osób (jeżeli akceptacja jest wymagana)

- Metryka musi zawierać:
    - Informacje o sposobie weryfikacji dokumentu
        - Datę dokonania weryfikacji
        - Imiona i nazwiska osób dokonujących weryfikacji
        - Zajmowane stanowiska i role pełnione w projekcie
        - Dane kontaktowe (np. adresy poczty elektronicznej, telefony)
    - Informacje o osobie odpowiedzialnej za nadzorowanie projektu, w ramach którego przygotowywana jest dokumentacja:
        - Imiona i nazwiska
        - Zajmowane stanowiska lub role pełnione w projekcie
        - Dane kontaktowe (np. adresy poczty elektronicznej, telefony)

Prawa autorskie

- Sekcja musi zawierać informacje o ochronie praw autorskich

Zastrzeżenia

- Sekcja musi zawierać informacje dotyczące poufności dokumentu

Indeksy

- Sekcja musi zawierać spis treści
- Sekcja musi zawierać:
    - Spis rysunków
    - Spis tabel
- Sekcja może zawierać inne indeksy

Słowniki

- Sekcja musi zawierać:
    - Słownik pojęć, skrótów, określeń i zwrotów używanych w dokumencie. Jeśli opisywane pojęcie jest skrótem, słownik musi zawierać rozwinięcie skrótu. Jeśli pojęcie jest słowem obcym, słownik musi zawierać tłumaczenie słowa na język polski.
- Sekcja musi zawierać:
    - Opis symboli graficznych wykorzystywanych w rysunkach.

Konwencje typograficzne

- Sekcja musi zawierać opis sposobu oznaczania charakterystycznych treści dokumentu, np.
    - Wszystkie słowa obcego pochodzenia piszemy *kursywą*;
    - Wszystkie nazwy komponentów piszemy **czcionką pogrubioną**;
    - Wszystkie fragmenty komunikacji z terminalem zawarte są w szarym polu otoczonym czarną ramką;
    - Wszelkie przykłady komunikacji z systemem operacyjnym opisywane są czcionką regularną.
    - Wyjątkowo istotne uwagi przedstawiono w ramce z wykrzyknikiem.

Wstęp

- Sekcja musi zawierać:
    - Cel opracowania dokumentu
    - Informację o dokumentach powiązanych lub referencje do innych dokumentów, których treść może mieć znaczenie w kontekście zawartości tego konkretnego dokumentu
- Sekcja może zawierać:
    - Określenie docelowych odbiorców dokumentu
    - Streszczenie dokumentu, opisujące pokrótce zawartość dalszych sekcji

Założenia i wymagania

Sekcja musi zawierać informacje o przedłożonych wymaganiach określonych w OPZ oraz założeniach przyjętych w ramach tworzenia projektu.

- Sekcja musi zawierać:
    - Wymagania ogólne
    - Założenia ogólne
- Sekcja musi zawierać:
    - Wymagania i założenia szczegółowe, np. w zakresie:
        - Cech funkcjonalnych rozwiązania
        - Cech ergonomicznych rozwiązania
        - Parametrów niezawodnościowych
        - Parametrów wydajnościowych
        - Utrzymania rozwiązania
        - Wdrożenia rozwiązania
        - Interfejsów komunikacyjnych oraz metod interakcji
        - Parametrów fizycznych
        - Ograniczeń
    - Inne wymagania i założenia specyficzne dla opisywanego rozwiązania, nie ujęte w żadnej z powyższych kategorii

Zakres projektu

- Sekcja musi opisywać:
    - Zakres projektowanego rozwiązania;
    - Zasięg rozwiązania – definiujący rozległość rozwiązania (ulokowanie komponentów w poszczególnych ośrodkach przetwarzania).

Definicja środowisk

- Sekcja musi zawierać definicje i opis projektowanych środowisk (o ile dotyczy), z wyszczególnieniem podstawowych zadań realizowanych przez każde środowisko, np.
    - Produkcyjne

- Akceptacyjne
- Testowe
- Deweloperskie

Rozwiązanie techniczne

Sekcja opisuje konkretne rozwiązanie techniczne w odniesieniu do każdego ze zdefiniowanych środowisk oraz komponentów sprzętu komputerowego i oprogramowania oraz jego konfigurację i integrację z infrastrukturą Zamawiającego.

Dokument musi zawierać opis wszystkich zagadnień technicznych, które można zdefiniować na etapie projektowania.

Zagadnienia mogą być dopracowane i uszczegółowione podczas etapu wdrożenia rozwiązania. Wówczas wszelkie dokonane w nich zmiany względem dokumentacji projektowej będą uwzględnione w dokumentacji powykonawczej.

- Muszą być opisane (o ile mają zastosowanie):
  - Architektura logiczna rozwiązania
    - Rozmieszczenie komponentów zwirtualizowanych (jeśli występują)
  - Budowy fizyczna
    - Rozmieszczenie komponentów w środowiskach fizycznych
  - Wykaz komponentów użytych do budowy rozwiązania (wybór urządzeń/oprogramowania), np:
    - Serwery,
    - zasoby dyskowe,
    - Komponenty sieci LAN,WAN,DWDM
    - Komponenty bezpieczeństwa komunikacji (zapory sieciowe),
    - Komponenty równoważące ruch sieciowy,
    - System backupu,
    - Systemy operacyjne,
    - Bazy danych,
    - Aplikacje,
    - Konsole do zarządzania serwerami,
    - Inne oprogramowanie
  - Architektura sieciowa i połączenia
    - Schemat fizyczny połączeń w sieci LAN//WAN/DWDM
    - Opis planowanego/przewidywanego obciążenia poszczególnych sieci przez komunikację w systemie,
    - Adresacja,
    - Nazwy w systemie DNS,
    - Źródła i sposób synchronizacji czasu,
  - Wytyczne konfiguracyjne dla poszczególnych komponentów rozwiązania.

Integracja

- Punkty styku oraz sposób integracji z innymi rozwiązaniami posiadanymi przez Zamawiającego,
    - Wykaz integrowanych systemów (min. Active Directory, sieć LAN, itp.),
    - Koncepcja rozwiązania.

Bezpieczeństwo

- Opis konfiguracji mechanizmów bezpieczeństwa dla wszystkich komponentów:
    - Wykorzystane mechanizmy ochrony komunikacji,
    - Sposób uwierzytelniania użytkowników,
    - Uprawnienia dla ról, użytkowników, grup,
    - Mechanizmy szyfrowania,
- Sposób tworzenia kopii zapasowych rozwiązania
    - Koncepcja – w szczególność sposób zabezpieczenia poszczególnych komponentów oraz replikacji danych pomiędzy ośrodkami przetwarzania,
    - Wymagane usługi,
    - Definicje podstawowych parametrów polityk kopiowania danych (np. harmonogramu kopiowania),
- Sposób odtwarzania systemów z kopii – koncepcja.

Zarządzanie

- Wykaz wykorzystywanych mechanizmów zarządzania,
- Opis sposobu zrządzania rozwiązaniem.

4.3.3. Dokumentacja Testowa

Niniejsza dokumentacja opisuje standard tworzenia Planu Testów Akceptacyjnych oraz Scenariuszy Testów Akceptacyjnych, które będą przygotowywane dla wszystkich komponentów sprzętu komputerowego i oprogramowania. Plan Testów Akceptacyjnych będzie dokumentował działania, jakie należy wykonać, aby uzyskać potwierdzenie, że wdrożenie osiągnęło zamierzone cele i funkcjonalności.

Scenariusze Testów Akceptacyjnych muszą być ściśle powiązane z Planu Testów Akceptacyjnych i opisywać szczegółowo sposób weryfikacji wymagań postawionych w OPZ oraz w dokumentacji Projektowej.

Dokumentacja testowa może ulec aktualizacji na etapie wdrożenia pod warunkiem, że Zamawiający wyrazi na to zgodę.

4.3.4. Plan Testów Akceptacyjnych

Dokument zostanie przygotowany w celu:

- ustanowienia standardu tworzenia Planów Testów Akceptacyjnych Systemu,
- dostarczenia autorom Planów Testów Akceptacyjnych dla dostarczonego sprzętu komputerowego i oprogramowania do których należy się stosować podczas tworzenia Planów Testów Akceptacyjnych Systemu,
- budowania zestawu Planu Testów Akceptacyjnych,
- opracowywania Scenariuszy Testów Akceptacyjnych,
- zapewnienia kompletności tworzonych Planów Testów Akceptacyjnych.

1. Struktura Procedury Testowej

Struktura Procedury Testowej jest uniwersalna i będzie miała zastosowanie do wszystkich komponentów sprzętu komputerowego i oprogramowania wdrażanych w ramach projektu. W szczególności będzie służyła do budowy Planu Testów Akceptacyjnych i Scenariuszy Testów Akceptacyjnych.

2. Procedura Testowa składa się następujących sekcji:

- identyfikacji wdrażanego komponentu sprzętu komputerowego i oprogramowania,
- wykazu czynności przygotowawczych,
- wykazu scenariuszy testowych,
- wykazu czynności końcowych.

3. Identyfikacja wdrażanego systemu

W sekcji identyfikacji wdrażanego systemu dokumentowane są dane ewidencyjne, dla którego tworzony jest Plan Testów Akceptacyjnych takie jak nazwa komponentu sprzętu komputerowego i oprogramowania oraz jego krótki opis.

4. Wykaz czynności przygotowawczych Procedury Testowej

W sekcji opisującej czynności przygotowawcze należy zidentyfikować a następnie uporządkować według kolejności ich wykonywania wszystkie czynności, jakie należy przeprowadzić przed przystąpieniem do testów tj. przed wykonywaniem scenariuszy testowych. Sekcja czynności przygotowawczych Procedury Testowej jest wypełniana tylko w takim przypadku, gdy czynności przygotowawcze mają zastosowanie w danej Procedurze Testowej.

Czynności przygotowawcze muszą obejmować między innymi takie zadania jak:

- weryfikacja dostępności raportu z testów umożliwiającego rejestrowanie przebiegu i wyników wykonania Procedury Testowej,
- weryfikacja poprawności instalacji i konfiguracji sprzętu i oprogramowania podlegającego testom,
- weryfikacja zasobów niezbędnych do przeprowadzenia i udokumentowania testów,

- weryfikacja oprogramowania niepodlegającego testom, ale niezbędnego do prawidłowego przeprowadzenia testów,
- weryfikacja użytkowników i ich uprawnień systemowych niezbędnych do wykonania testów,
- weryfikacja dostępności i poprawności danych testowych,
- weryfikacja dostępności narzędzi do weryfikacji wyników poszczególnych testów (np. skrypty, narzędzia pomiarowe, narzędzia monitorujące, narzędzia administracyjne itp.).

Przebieg i rezultaty wykonania czynności przygotowawczych dokumentowane są w raporcie z wykonania Procedury Testowej (stanowią integralną część dokumentacji z wykonanych testów).

5. Wykaz scenariuszy testowych Procedury Testowej

W sekcji przedstawiającej wykaz scenariuszy testowych należy zidentyfikować i uporządkować, według kolejności ich wykonywania, wszystkie scenariusze testowe przewidziane do realizacji w ramach Procedury Testowej. Następnie każdy scenariusz testowy należy opisać zgodnie z poniższymi wytycznymi.

Podczas identyfikacji scenariuszy testowych należy kierować się zasadą, że każdy scenariusz testowy to zbiór przypadków (kroków) testowych, których wykonanie jest potrzebne do sprawdzenia poprawności działania systemu w określonym zakresie. Każdy scenariusz testowy powinien być odzwierciedleniem dokładnie określonej funkcjonalności systemu lub sprawdzeniem cech niefunkcjonalnych takich jak: wydajność, niezawodność, bezpieczeństwo itp.

4.3.5. Scenariusze testowe

1. Struktura Scenariuszy Testowych

Opis każdego scenariusza testowego musi posiadać następującą strukturę:

- identyfikację scenariusza testowego,
- wykaz czynności przygotowawczych,
- wykaz przypadków testowych,
- wykaz czynności końcowych.

2. Identyfikacja scenariusza testowego

W sekcji identyfikacji scenariusza testowego dokumentowane są następujące dane ewidencyjne scenariusza testowego:

- unikalny identyfikator (w ramach Planu Testów Akceptacyjnych Systemu) i nazwa scenariusza testowego,
- opis scenariusza testowego przedstawiający cel/cele jego wykonania,
- typ scenariusza (rodzaj testu wykonywanego w ramach danego scenariusza np. testy funkcjonalne, testy wydajnościowe, testy niezawodności, testy bezpieczeństwa itp.).

Wykaz czynności przygotowawczych scenariusza testowego

W sekcji opisującej czynności przygotowawcze scenariusza testowego należy zidentyfikować a następnie uporządkować, według kolejności ich wykonywania, wszystkie czynności, jakie powinny być wykonane przed przystąpieniem do realizacji scenariusza testowego tj. przed wykonywaniem pierwszego przypadku testowego. Sekcja czynności przygotowawczych scenariusza testowego jest wypełniana tylko w takim przypadku, gdy te czynności mają zastosowanie w danym scenariuszu testowym.

Czynności przygotowawcze scenariusza testowego są uzupełnieniem czynności przygotowawczych Procedury Testowej. Obejmują one te czynności, które nie mogą być wykonane w ramach czynności przygotowawczych Procedury Testowej, gdyż:

- uniemożliwiłby wykonanie poprzedzających scenariuszy testowych lub zafałszowałyby wynik wykonania tych scenariuszy;
- uniemożliwiłby wykonanie następnych scenariuszy testowych lub zafałszowałby wynik wykonania tych scenariuszy; w tym przypadku, w ramach czynności końcowych danego scenariusza testowego należy wykonać odpowiednie działania eliminujące efekt wykonania czynności przygotowawczych w celu umożliwienia wykonania następnych scenariuszy testowych.

Wykaz przypadków testowych scenariusza testowego

W sekcji przedstawiającej wykaz przypadków testowych scenariusza testowego należy zidentyfikować i uporządkować, według kolejności ich wykonywania, wszystkie przypadki testowe przewidziane do realizacji w ramach danego scenariusza testowego. Następnie każdy przypadek testowy należy opisać zgodnie z poniższymi wytycznymi.

Podczas identyfikacji przypadków testowych należy kierować się zasadą, że każdy przypadek testowy jest określony przez: zbiór danych wejściowych, warunków początkowych oraz oczekiwanych wyników i warunków końcowych i jest on tworzony w celu realizacji określonej funkcjonalności i/lub w celu weryfikacji zgodności z określonym wymaganiem.

Struktura przypadku testowego

a. Opis każdego przypadku testowego posiada następującą strukturę:

- identyfikacja przypadku testowego,
- wykaz czynności przygotowawczych,
- warunki początkowe,
- zestaw danych testowych,
- lista weryfikowanych wymagań/funkcjonalności,

- wykaz kroków przypadku testowego,
- oczekiwany rezultat wykonania przypadku testowego,
- metodę weryfikacji poprawności rezultatu wykonania przypadku testowego,
- wykaz czynności końcowych.

b. Identyfikacja przypadku testowego

W sekcji identyfikacji przypadku testowego dokumentowane są następujące dane ewidencyjne przypadku testowego:

- unikalny identyfikator (w ramach Planu Testów Akceptacyjnych) i nazwa przypadku testowego.
- opis przypadku testowego przedstawiający cel jego wykonania.

c. Wykaz czynności przygotowawczych przypadku testowego

Analogicznie jak w przypadku czynności przygotowawczych scenariusza testowego.

d. Warunki początkowe przypadku testowego

W sekcji opisującej warunki początkowe przypadku testowego dokumentuje się wszystkie warunki, jakie muszą być spełnione, aby przystąpić do wykonywania kroków przypadku testowego. Spełnienie tych warunków powinno być zapewnione poprzez poprawne wykonanie:

- czynności przygotowawczych Procedury Testowej,
- czynności przygotowawczych oraz czynności końcowych wszystkich poprzedzających scenariuszy i przypadków testowych.

e. Zestawy danych testowych dla przypadku testowego

W niniejszej sekcji należy opisać wszystkie zestawy danych testowych wykorzystywane w krokach danego przypadku testowego. Dla każdego zestawu należy podać:

- unikalny identyfikator (w ramach Planu Testów Akceptacyjnych).
- charakterystykę danych opisywanego zestawu (opcjonalnie - np. w przypadki pojedynczych danych wprowadzanych przez testera do systemu poprzez GUI; obowiązkowo – np. w przypadku dużego wolumenu danych wprowadzanych do systemu poprzez automatyczny import).
- nazwy i konkretne wartości danych testowych (alternatywnie: dołączyć zbiór z zestawem danych testowych, jako załącznik lub wskazać lokalizację zbioru w repozytorium).

f. Lista weryfikowanych wymagań/funkcjonalności

Każdy przypadek testowy ma na celu weryfikację zgodności z określonym wymaganiem i/lub weryfikację poprawności określonej funkcjonalności. W niniejszej sekcji należy wskazać wymagania i/lub funkcjonalności weryfikowanych (testowanych) w ramach danego przypadku testowego. Poprawny wynik wykonania danego przypadku testowego jest tożsamy z pozytywną weryfikacją wymagań i/lub

funkcjonalności powiązanych z danym przypadkiem testowym o ile te wymagania i/lub funkcjonalności nie są powiązane z jeszcze innymi przypadkami testowymi. Jeśli istnieje powiązanie z innymi przypadkami testowymi, to pozytywna weryfikacja określonego wymagania/funkcjonalności następuje w przypadku pozytywnego wykonania wszystkich przypadków testowych powiązanych z danym wymaganiem/funkcjonalnością.

g. Wykaz kroków przypadku testowego

W sekcji przedstawiającej wykaz kroków przypadku testowego należy zidentyfikować i uporządkować, według kolejności ich wykonywania, wszystkie czynności, jakie należy przeprowadzić w celu wykonania danego przypadku testowego. Dla każdego kroku należy wskazać identyfikator odpowiedniego zestawu danych testowych, o ile w danym kroku następuje wprowadzenie danych testowych do systemu.

h. Oczekiwany rezultat wykonania przypadku testowego

Dla każdego przypadku testowego należy opisać oczekiwany rezultat wykonania danego przypadku testowego (wykonania wszystkich kroków przypadku testowego). Zgodność oczekiwanego rezultatu wykonania przypadku testowego z rzeczywistym rezultatem otrzymanym po wykonaniu danego przypadku testowego jest tożsamy z pozytywnym wynikiem wykonania danego przypadku testowego.

i. Metoda weryfikacji poprawności rezultatu wykonania przypadku testowego

W niniejszej sekcji należy opisać metodę weryfikacji rezultatu wykonania przypadku testowego z rezultatem oczekiwanym. W szczególności w przypadku analizy dużego wolumenu danych wynikowych lub zebranych pomiarów, należy dokładnie wskazać narzędzia (np. skrypty, narzędzia pomiarowe, narzędzia monitorujące, narzędzia administracyjne itp.) niezbędne do wykonania weryfikacji oraz sposób i wyniki ich użycia.

Wykaz czynności końcowych przypadku testowego

W sekcji opisującej czynności końcowe przypadku testowego należy zidentyfikować a następnie uporządkować według kolejności wykonywania wszystkie czynności, jakie należy wykonać po zakończeniu wykonywania przypadku testowego tj. po wykonaniu ostatniego kroku przypadku testowego. Sekcja czynności końcowych przypadku testowego jest wypełniania tylko w takim przypadku, gdy czynności końcowe mają zastosowanie w danym przypadku testowym.

Czynności końcowe przypadku testowego obejmują te czynności, bez których wykonanie następnych przypadków i scenariuszy testowych byłoby niemożliwe lub wynik ich wykonania byłby zafałszowany lub które wynikają z wymogów polityk bezpieczeństwa.

Wykaz czynności końcowych scenariusza testowego

Analogicznie jak w przypadku czynności końcowych przypadku testowego.

Wykaz czynności końcowych Procedury Testowej

W sekcji opisującej czynności końcowe Procedury Testowej należy zidentyfikować a następnie uporządkować według kolejności wykonywania wszystkie czynności, jakie należy wykonać po zakończeniu wykonywania ostatniego scenariusza testowego. Sekcja czynności końcowych Procedury Testowej jest wypełniana tylko w takim przypadku, gdy czynności końcowe mają zastosowanie w danej Procedurze.
W szczególności czynności końcowe mogą obejmować:

- Zabezpieczenie/usunięcie danych wrażliwych.
- Usunięcie/zablokowanie użytkowników i uprawnień w celu eliminacji ryzyka nieuprawnionego dostępu i użytkowania środowiska testowego.
- Zwolnienie limitowanych zasobów i narzędzi niezbędnych do realizacji innych zadań.
- Przywrócenie standardowych ustawień zasobów, dla których na czas testów nastąpiła rekonfiguracja.
- Archiwizację danych, konfiguracji i logów, w celu dalszej analizy.

4.3.6. Dokumentacja Powykonawcza, która powstanie jako uaktualnienie Projektu Wykonawczego wdrożenia dostarczanych elementów SZIRS,

Streszczenie
Dokument opisuje standard dokumentacji powykonawczej dla dostarczonego sprzętu komputerowego i oprogramowania oraz jego konfigurację i integrację z infrastrukturą Zamawiającego
Opis
Cechy ogólne

- Dokumentacja musi być przygotowana zgodnie z szablonem ustalonym dla całej organizacji lub wyodrębnionego projektu.
- Kolejne sekcje dokumentacji muszą być numerowane w sposób kontekstowy – numeracja kolejnych podsekcji musi być poprzedzona numerem sekcji wyższej.
- Opis sekcji przedstawiono w kolejności, w jakiej muszą one występować w dokumencie.
- Główną ideą opracowania dokumentacji powykonawczej jest przedstawienie opisu zbudowanego środowiska w sposób jak najlepiej odzwierciedlający rzeczywistość. Wsadem do dokumentacji powykonawczej mogą być elementy, stworzonej wcześniej, dokumentacji projektowej – zmodyfikowane, uzupełnione i uszczegółowione w sposób urealniający stan systemu i prezentujący rozwiązanie w jego ostatecznej, zaakceptowanej i używanej formie – tak, jak ono rzeczywiście wygląda.

Strona tytułowa

- Musi zawierać co najmniej następujące informacje:
    - Tytuł dokumentu

    - Nazwę lub numer tematu (zagadnienia)
    - Nazwę projektu
    - Informacje o autorach dokumentu:
        - Imiona, Nazwiska
        - Zajmowane stanowiska lub role pełnione w projekcie
        - Nazwę organizacji
- Strona tytułowa może zawierać inne, dodatkowe informacje, zgodnie z ustalonym szablonem, np.:
    - Identyfikator projektu, identyfikator dokumentu w projekcie lub inne identyfikatory
    - Dodatkowe informacje precyzujące temat zagadnienia, np. nazwę podprojektu, określenie konkretnego tematu lub zagadnienia
    - Nazwę organizacji , nazwę jednostki organizacyjnej
    - Adres organizacji lub jednostki organizacyjnej
    - Bardziej szczegółowe informacje o autorach dokumentu:
        - Telefony kontaktowe
        - Adresy poczty elektronicznej

Metryka

- Metryka dokumentu musi zawierać co najmniej następujące informacje:
    - Określenie aktualnej wersji dokumentu
    - Datę publikacji dokumentu
    - Bardziej szczegółowe informacje o autorach dokumentu (jeśli nie były określone na stronie tytułowej):
        - Telefony kontaktowe
        - Adresy poczty elektronicznej
    - Historię zmian w dokumencie, zawierającą co najmniej następujące pola:
        - Wersję
        - Datę
        - Imiona i nazwiska autorów zmian
        - Krótki opis dokonanych zmian
    - Informację o akceptacji dokumentu – miejsca na podpisy właściwych osób (jeżeli akceptacja jest wymagana)
- Metryka musi zawierać:
    - Informacje o sposobie weryfikacji dokumentu
        - Datę dokonania weryfikacji
        - Imiona i nazwiska osób dokonujących weryfikacji
        - Zajmowane stanowiska i role pełnione w projekcie
        - Dane kontaktowe (np. adresy poczty elektronicznej, telefony)

- Informacje o osobie odpowiedzialnej za nadzorowanie projektu w ramach którego przygotowywana jest dokumentacja:
  - Imiona i nazwiska
  - Zajmowane stanowiska lub role pełnione w projekcie
  - Dane kontaktowe (np. adresy poczty elektronicznej, telefony)

Prawa autorskie

- Sekcja musi zawierać informacje o ochronie praw autorskich

Zastrzeżenia

- Sekcja musi zawierać informacje dotyczące poufności dokumentu

Indeksy

- Sekcja musi zawierać spis treści
- Sekcja musi zawierać:
  - Spis rysunków
  - Spis tabel
- Sekcja może zawierać inne indeksy

Słowniki

- Sekcja musi zawierać:
  - Słownik pojęć, skrótów, określeń i zwrotów używanych w dokumencie. Jeśli opisywane pojęcie jest skrótem, słownik musi zawierać rozwinięcie skrótu. Jeśli pojęcie jest słowem obcym, słownik musi zawierać tłumaczenie słowa na język polski.
- Sekcja musi zawierać:
  - Opis symboli graficznych wykorzystywanych w rysunkach.

Konwencje typograficzne

- Sekcja musi zawierać opis sposobu oznaczania charakterystycznych treści dokumentu, np.
  - Wszystkie słowa obcego pochodzenia piszemy *kursywą*;
  - Wszystkie nazwy komponentów piszemy **czcionką pogrubioną**;
  - Wszystkie fragmenty komunikacji z terminalem zawarte są w szarym polu otoczonym czarną ramką;
  - Wszelkie przykłady komunikacji z systemem operacyjnym opisywane są czcionką regularną.
  - Wyjątkowo istotne uwagi przedstawiono w ramce z wykrzyknikiem.

Wstęp

- Sekcja musi zawierać:
  - Cel opracowania dokumentu
  - Informację o dokumentach powiązanych lub referencje do innych dokumentów, których treść może mieć znaczenie w kontekście zawartości tego konkretnego dokumentu

- Sekcja może zawierać:
    - Określenie docelowych odbiorców dokumentu
    - Streszczenie dokumentu, opisujące pokrótce zawartość dalszych sekcji

Zakres i zasięg rozwiązania

- Sekcja musi opisywać:
    - Zakres zbudowanego rozwiązania;
    - Zasięg zbudowanego rozwiązania – opisujący rozległość rozwiązania (ulokowanie komponentów w poszczególnych ośrodkach).

Definicja środowisk

- Sekcja musi zawierać definicję i opis zbudowanych środowisk, z wyszczególnieniem podstawowych zadań realizowanych przez każde środowisko, np.
    - Produkcyjne
    - Akceptacyjne
    - Testowe
    - Deweloperskie

Rozwiązanie techniczne

Sekcja opisuje konkretne rozwiązanie techniczne w odniesieniu do każdego z komponentów sprzętu komputerowego i oprogramowania oraz jego konfigurację i integrację z infrastrukturą Zamawiającego.

Dokument musi zawierać opis wszystkich zagadnień technicznych stworzonego rozwiązania.

- Dla każdego środowiska muszą być opisane (o ile mają zastosowanie):
    - Wynikowa architektura logiczna rozwiązania
        - Rozmieszczenie poszczególnych komponentów w przestrzeni całego rozwiązania
    - Budowy fizyczna
        - Fizyczne rozmieszczenie komponentów w wyodrębnionych środowiskach operacyjnych
    - Cechy funkcjonalne uzyskanego rozwiązania
    - Cechy ergonomiczne rozwiązania
    - Parametry niezawodnościowe
    - Parametry wydajnościowe
    - Sposób utrzymania rozwiązania
    - Interfejsy komunikacyjne oraz metod interakcji
    - Parametry fizyczne
    - Ograniczenia
    - Komponenty użyte do budowy rozwiązania, np:
        - Serwery,
        - zasoby dyskowe,

        - Komponenty sieci LAN,WAN,DWDM
        - Komponenty bezpieczeństwa komunikacji (zapory sieciowe),
        - Komponenty równoważące ruch sieciowy,
        - System backupu,
        - Systemy operacyjne,
        - Bazy danych,
        - Aplikacje,
        - Konsole do zarządzania serwerami,
        - Inne oprogramowanie
    - Architektura sieciowa i połączenia
        - Schemat fizyczny połączeń w sieci LAN//WAN/DWDM
        - Opis planowanego/przewidywanego obciążenia poszczególnych sieci przez komunikację w systemie,
        - Adresacja,
        - Nazwy w systemie DNS,
        - Źródła i sposób synchronizacji czasu,
    - Konfiguracja dla poszczególnych komponentów rozwiązania.

Integracja

- Sekcja musi opisywać punkty styku oraz sposób integracji zbudowanego rozwiązania z innymi rozwiązaniami. Musi zawierać co najmniej:
    - Wykaz zintegrowanych systemów (min. Active Directory, sieć LAN, itp.),
    - Opis użytych rozwiązań integracyjnych

Bezpieczeństwo

- Opis konfiguracji mechanizmów bezpieczeństwa dla wszystkich komponentów:
    - Wykorzystane mechanizmy ochrony komunikacji
    - Sposób uwierzytelniania użytkowników
    - Uprawnienia dla ról, użytkowników, grup
    - Mechanizmy szyfrowania
- Sposób tworzenia kopii zapasowych rozwiązania
    - Sposób kopiowania danych poszczególnych komponentów
    - Harmonogramu kopiowania
- Sposób odtwarzania systemu z kopii.

Zarządzanie

- Wykaz wykorzystywanych mechanizmów zarządzania
- Opis sposobu zrządzania komponentami rozwiązania

Załączniki

- Wykaz załączników do dokumentacji powykonawczej

4.3.7. Procedury operacyjne i administracyjne

Streszczenie

Dokument opisuje standard tworzenia procedur operacyjnych i administracyjnych dostarczonego sprzętu komputerowego i oprogramowania. Lista procedur stanowi jedynie przykład i zostanie uszczegółowiona na etapie realizacji projektu.

Opis

Niniejszy dokument opisuje charakterystyczne zagadnienia proceduralne oraz przykłady zastosowań procedury.

- Procedura musi być przygotowana w oparciu o *Szablon procedury*.
- Realizacja procedury musi być udokumentowana *Raportem wykonania procedury*, którego szablon zawarty jest w *Szablon procedury*.

Poniżej zawarte zostały główne zagadnienia związane z poszczególnymi komponentami sprzętu komputerowego i oprogramowania.

Serwery

Sytuacja początkowa

- Przykładowe sytuacje początkowe w procedurze:
    - konieczność aktualizacji mikrokodu;
    - konieczność wymiany komponentów sprzętowych

Warunki użycia

- Przykładowe warunki użycia procedury:
    - dostępność innego serwera (węzła zastępczego) w klastrze;
    - dostępność innych serwerów w farmie;
    - system operacyjny na serwerze został wcześniej zatrzymany;
    - środowisko wirtualizujące na serwerze zostało wcześniej zatrzymane.

Komponenty sieci LAN

Sytuacja początkowa

- Przykładowe sytuacje początkowe w procedurze:
    - konieczność wyłączenia obu linii zasilania przełączników LAN.

4.4. Wymagania w zakresie wdrożenia

4.4.1. Wymagania w zakresie dostawy:

1. Wykonawca jest zobowiązany do dostarczenia Sprzętu do miejsca wskazanego przez Zamawiającego. Adresy miejsca dostawy sprzętu zostanie przekazane Wykonawcy w dniu zawarcia Umowy, na adres poczty elektronicznej wskazany w Umowie.

2. Dostawa i wszelkie czynności z nią związane realizowane będą przez Wykonawcę w Dni Robocze w godzinach 8:00 - 16:00.
3. Przed rozpoczęciem dostaw, Wykonawca zobowiązany jest dostarczyć Zamawiającemu pisemnie lub drogą elektroniczną na adres wskazany przez Zamawiającego, z minimum 2-dniowym wyprzedzeniem, powiadomienie zawierające co najmniej:

- datę, godzinę rozpoczęcia dostawy,
- szczegółowy wykaz Sprzętu dostarczanego w ramach dostawy z wyszczególnieniem nazw oraz liczby oraz numerów seryjnych,
- listę osób realizujących dostawę z wyszczególnieniem ich imienia i nazwiska oraz markę, model i numer rejestracyjny samochodu, którym zostanie dostarczony Sprzęt.

4. W przypadku niedotrzymania przez Wykonawcę terminu powiadomienia o dostawie, o którym mowa w ust. 1c., Zamawiający ma prawo odmówić odbioru dostawy. W takim wypadku następuje ponowne wdrożenie procedury przewidzianej w pkt 1.c.
5. Wykonawca zobowiązuje się do poniesienia wszelkich kosztów dostawy do miejsca wskazanego przez Zamawiającego, w szczególności kosztów opakowania, transportu.
6. Wykonawca po wykonaniu Wdrożenia zobowiązany jest do uprzątnięcia wszelkich opakowań wynikających z realizacji Umowy.

4.4.2. Wymagania w zakresie Wdrożenia:

1. Instalacja, konfiguracja i integracja ze środowiskiem Zamawiającego wszystkich dostarczonych komponentów Sprzętu o Oprogramowania ,
2. aktualizacja oprogramowania wewnętrznego (firmware) na wszystkich dostarczanych urządzeniach,
3. dostarczenie i zainstalowanie niezbędnych licencji i oprogramowania,
4. dostarczenie okablowania wymaganego do podłączenia dostarczonego sprzętu i wykonanie podłączeń,
5. przeprowadzenia wyżej wymienionych prac bez zakłóceń pracy Infrastruktury Zamawiającego.
6. Posadowienie na zainstalowanym Sprzęcie i Oprogramowaniu Oprogramowania Dedykowanego systemu SZIRS.
7. Wykonanie dokumentacji projektowej i testowej
8. Przeprowadzenie testów Sprzętu i Oprogramowania oraz Oprogramowania Dedykowanego systemu SZIRS zgodnie z przygotowana Dokumentacją Testową.

4.5. Wymagania w zakresie warsztatów

Wymagania Ogólne

Wykonawca przedstawi Zamawiającemu na co najmniej 7 dni przed rozpoczęciem warsztatów, do akceptacji:

- miejsce przeszkolenia
- zakres przeszkolenia
- agendę
- kwalifikacje Wykładowcy
- materiały szkoleniowe.

Warsztaty będą prowadzone w języku polskim.
Wykonawca do realizacji warsztatów skieruje osobę posiadającą kwalifikacje i odpowiednią wiedzę do przeprowadzenia warsztatów.
Wykonawca zobowiązuje się do zapewnienia miejsca warsztatów wraz ze stanowiskiem komputerowym dla każdego uczestnika oraz wszelkie niezbędne oprogramowanie,
Każdy z uczestników warsztatów otrzyma komplet materiałów szkoleniowych w języku polskim (w formie papierowej oraz elektronicznej). Zamawiający dopuszcza przekazanie materiałów szkoleniowych w języku angielskim pod warunkiem, że producent Sprzętu lub Oprogramowania nie udostępnia materiałów w j. polskim.
Wykonawca zapewni salę szkoleniową na terenie Warszawy wraz z wyżywieniem (jeden gorący posiłek składający się z dwóch dań dziennie oraz kawa, herbata i zimne napoje podczas trwania przeszkoleń).
Każdy z uczestników warsztatów otrzyma potwierdzenie udziału w warsztatach.
Wszelkie koszty warsztatów ponosi Wykonawca.
Wykonawca przedstawi do akceptacji i uzgodni z Zamawiającym program warsztatów wraz z harmonogramem, w terminie do 10 dni kalendarzowych od daty zawarcia Umowy. Wykonawca zobowiązany jest do zrealizowania warsztatów do momentu zakończenia Wdrożenia.
Na wniosek Zamawiającego, warsztaty mogą odbyć się w formie zdalnej (online).
Zamawiający powiadomi o tym fakcie najpóźniej na 7 dni przed datą rozpoczęcia warsztatów. W takim przypadku ust. d,f,g nie mają zastosowania.
W przypadku warsztatów w formie zdalnej zachowana musi być interaktywna forma warsztatów. Uczestnicy w czasie rzeczywistym muszą widzieć i słyszeć wykładowcę, móc zadawać pytania i wyjaśniać wątpliwości oraz wykonywać ćwiczenia praktyczne. Wykładowca musi udostępniać na bieżąco na ekranie materiały szkoleniowe. Uczestnicy muszą również widzieć i słyszeć siebie wzajemnie. Wykonawca musi w tym celu zapewnić platformę szkoleniową dostępną dla uczestników warsztatów za pośrednictwem sieci Internet, działającą na komputerach wyposażonych w system operacyjny Microsoft Windows 7/10/11 wyposażonych w urządzenia audio i video (słuchawki/mikrofon/kamera internetowa).

W przypadku warsztatów w formie zdalnej Wykonawca najpóźniej na dwa dni przed datą rozpoczęcia przekaże drogą mailową, wszelkie dane wymagane do podłączenia się do platformy szkoleniowej (np. loginy, hasła, link dostępowy itp.) oraz instrukcję użytkowania platformy.

Wymagania w zakresie Sprzętu i Oprogramowania:
Warsztaty będą obejmowały co najmniej zagadnienia z zakresu administracji, konfiguracji oraz zarządzania zaoferowanego Sprzętu i Oprogramowania.
Warsztaty odbędą się w dwóch turach o nienakładających się terminach, po maksymalnie 3 uczestników ze strony Zamawiającego w każdej turze. Każda tura warsztatów trwać będzie minimum 40 godzin, jednak nie więcej niż 8 godzin jednego dnia, dzień po dniu, w dni robocze.
Merytoryczna zawartość warsztatów w zakresie dostarczonego Sprzętu i Oprogramowania:

- administracja i użytkowanie zaoferowanego Sprzętu i Oprogramowania,
- omówienie architektury zaoferowanego rozwiązania,
- omówienie narzędzi administracyjnych (GUI, CLI),
- omówienie narzędzi monitorujących poszczególne komponenty,

Ćwiczenia praktyczne:

- konfiguracja poszczególnych komponentów Sprzętu i Oprogramowania,
- monitoring i zarządzanie, uprawnienia użytkowników,
- diagnostyka i rozwiązywanie problemów,
- optymalizacja wydajności.

Wymagania w zakresie Oprogramowania Dedykowanego systemu SZIRS:
Warsztaty będą obejmowały co najmniej zagadnienia z zakresu obsługi Oprogramowania Dedykowanego systemu SZIRS.
Warsztaty odbędą się w dwóch turach o nienakładających się terminach, po maksymalnie 10 uczestników ze strony Zamawiającego w każdej turze. Każda tura warsztatów trwać będzie minimum 32 godzin, jednak nie więcej niż 8 godzin jednego dnia, dzień po dniu, w dni robocze.
Merytoryczna zawartość warsztatów (w tym ćwiczenia) w zakresie dostarczonego Sprzętu i Oprogramowania:

- Architektura systemu SZIRS,
- Obsługa interfejsu użytkownika,
- Uruchamianie i dostosowywanie raportów BI,
- Zasilanie hurtowni danymi,
- Zarządzanie użytkownikami i uprawnieniami.

4.6. Wymagania co do osób realizujących zamówienie ze strony Wykonawcy

Wykonawca skieruje do realizacji zamówienia zespół w składzie i spełniający następujące wymagania, przy czym lista osób wraz z wykazanym doświadczeniem składana jest w terminie 3 dni od dnia zawarcia umowy.

1) **Senior Programista Backend – co najmniej 2 osoby:**

- udział w roli Seniora Programisty Backeend w projekcie wdrożenia systemu dedykowanego o budżecie co najmniej 500 000,00 brutto, nie wcześniej niż w ciągu ostatnich trzech lat przed upływem terminu składania ofert.

2) **Senior Programista Frontend – co najmniej 2 osoby:**

- udział w roli Seniora Programisty Frontend w projekcie wdrożenia systemu dedykowanego z wykorzystaniem technologii REACT, Angular lub VueJS, o budżecie co najmniej 500 000,00 brutto, nie wcześniej niż w ciągu ostatnich trzech lat przed upływem terminu składania ofert.

3) **Specjalista ETL – co najmniej 1 osoba:**

- Udział, w roli Specjalisty ETL lub Programisty procesów ETL, w projekcie wdrożenia systemu dedykowanego, o budżecie co najmniej 500 000,00 brutto, nie wcześniej niż w ciągu ostatnich trzech lat przed upływem terminu składania ofert.

4) **Analityk Biznesowy – co najmniej 2 osoby:**

- Udział, w roli Analityka biznesowego, w projekcie wdrożenia systemu dedykowanego, o budżecie co najmniej 3 000 000,00 brutto, nie wcześniej niż w ciągu ostatnich trzech lat przed upływem terminu składania ofert.

5) **Analityk Systemowy – co najmniej 1 osoba:**

- Udział, w roli Analityka systemowego, w projekcie wdrożenia systemu dedykowanego, o budżecie co najmniej 500 000,00 brutto, nie wcześniej niż w ciągu ostatnich trzech lat przed upływem terminu składania ofert.

6) **Tester Aplikacji – co najmniej 2 osoby:**

- Udział, w roli Testera, w projekcie wdrożenia systemu dedykowanego, o budżecie co najmniej 500 000,00 brutto, nie wcześniej niż w ciągu ostatnich trzech lat przed upływem terminu składania ofert.

Rola Testera nie może być współdzielona z rolą Programisty Backend/FrontEnd.

Zamawiający jest uprawniony na etapie realizacji do żądania dokumentów potwierdzających spełniania przez ww. osoby ww. wymagań.