ZP.272.16.2024 **Załącznik nr 1 do SWZ**

OPIS PRZEDMIOTU ZAMÓWIENIA
/OPZ/

w postępowaniu o udzielenie zamówienia na rozbudowę i wdrożenie środowiska kopii zapasowych Starostwa Powiatowego w Nowym Sączu oraz dostawę sprzętu komputerowego w ramach projektu pn.: „Cyberbezpieczny Powiat Nowosądecki".

1. Przedmiotem zamówienia jest rozbudowa i wdrożenie środowiska kopii zapasowych Starostwa Powiatowego w Nowym Sączu oraz dostawa sprzętu komputerowego w ramach projektu pn.: „Cyberbezpieczny Powiat Nowosądecki" współfinansowanego przez Unię Europejską w ramach Programu Operacyjnego Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (FERC), Priorytet II Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa.
2. Termin realizacji zamówienia:
   Część I: do 50 dni kalendarzowych od dnia zawarcia umowy.
   Część II: do 50 dni kalendarzowych od dnia zawarcia umowy.
3. Zasady dostawy:
   a) miejsce dostawy: siedziba Starostwa Powiatowego w Nowym Sączu, ul. Jagiellońska 33, 33-300 Nowy Sącz, II piętro,
   b) wykonawca jest zobowiązany poinformować zamawiającego na piśmie, mailowo lub telefonicznie o planowanym terminie dostawy co najmniej na 3 dni robocze przed tym terminem,
   c) dostawa zostanie zrealizowana w dniu roboczym w godzinach od 8.00 do 14.00,
   d) przedmiot zamówienia dostarczony będzie jednorazowo w zakresie danej części zamówienia,
   e) wykonawca jest zobowiązany do zrealizowania usług towarzyszących dostawie, takich jak transport, załadunek, rozładunek, wniesienie do pomieszczeń wskazanych przez przedstawicieli zamawiającego oraz wszelkich innych usług dodatkowych niezbędnych do prawidłowego wykonania zamówienia,
   f) wykonawca zobowiązany jest zainstalować dostarczony sprzęt w miejscu wskazanym przez przedstawiciela zamawiającego.
4. Dostarczane urządzenia i ich komponenty muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta. Koszty transportu do siedziby zamawiającego oraz koszty usług towarzyszących dostawie, o których mowa powyżej w pkt 3 lit. e) i f) ponosi wykonawca.
5. Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej, w języku polskim i/lub angielskim.
6. Wszystkie urządzenia muszą posiadać oznakowanie CE produktu albo spełniać normy równoważne. Wraz z dostawą należy dostarczyć poświadczoną przez wykonawcę kopię

certyfikatu CE dla oferowanego sprzętu lub dokumentu równoważnego, lub oświadczenia producenta.

7. Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230V ± 10%, 50 Hz.
8. Wszystkie przewody połączeniowe oraz inne akcesoria niezbędne do montażu urządzeń dostarcza wykonawca.
9. Miejscem instalacji sprzętu będzie siedziba zamawiającego w Nowym Sączu, ul. Jagiellońska 33, II piętro – serwerownia.
10. Oferowane produkty muszą zapewnić pełną kompatybilność z istniejącym środowiskiem Zamawiającego.
11. W trakcie realizacji przedmiotu zamówienia zamawiający wskaże osoby ze strony zamawiającego, odpowiedzialne za współpracę przy realizacji zadania.
12. Dostarczane elementy muszą być fabrycznie nowe i nieużywane w innych projektach informatycznych oraz pochodzić z autoryzowanego kanału sprzedaży producentów na rynek polski lub UE. Zamawiający wymaga w tym zakresie oświadczenia wykonawcy złożonego wraz z ofertą.
13. Wszystkie dostarczane urządzenia muszą znajdować się w ofercie producenta, na dzień składania ofert. Wykonawca nie może dostarczyć zmawiającemu urządzeń, modułów czy podzespołów wycofanych przez producenta z produkcji lub sprzedaży (tzw. End-of-sale).
14. Zamawiający zastrzega sobie możliwość sprawdzenia spełnienia wszystkich warunków lub wymagań, względem zamawianych urządzeń, modułów i podzespołów w tym gwarancji i pakietów serwisowych w polskim lub europejskim biurze producenta na podstawie numeru seryjnego. W przypadku niezgodności deklaracji wykonawcy z opinią producenta - zamawiający odmówi odbioru przedmiotu zamówienia, jako niezgodnego z zapisami/warunkami umowy. Zamawiający wymaga oświadczenia producentów sprzętu złożonego z ofertą, w przedmiocie objęcia gwarancją elementów dostawy. Dostarczany sprzęt musi być możliwy do jednoznacznego zidentyfikowania, zgodnie z formularzem produktowym stanowiącym integralną część formularza oferty.
15. We wszystkich pozycjach, w których występuje znak towarowy, patent, pochodzenie, nazwa własna towaru lub jego producenta, źródło lub szczególny proces, który charakteryzuje produkty dostarczane przez konkretnego wykonawcę, zamawiający dopuszcza możliwość dostawy produktów równoważnych, tj. o nie gorszych parametrach technicznych niż te, które posiadają produkty wskazane za pomocą znaku towarowego czy pochodzenia. Jeśli Zamawiający określa w niniejszej specyfikacji, że dany element ma posiadać określone cechy, to ten element musi efektywnie pracować z tymi cechami w instalowanej konfiguracji. Przykładowo, jeśli wymaga się dostarczenia modułów pamięci pracujących z daną prędkością, to te moduły muszą efektywnie pracować z taką prędkością, a nie mieć tylko taką teoretyczną możliwość w konfiguracji innej niż dostarczana.
16. Dodatkowe wymagania dotyczące zamówienia:
    a) Spełnienie wymagań okreslonych dla Części I zamówienia musi zostać potwierdzone w oświadczeniu wykonawcy oraz w oświadczeniu producenta/producentów sprzętu, złożonym przed podpisaniem umowy.

b) W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostanie u zamawiającego a wymiana dysku może być dokonana przez zamawiającego.

Część I zamówienia:

KODY CPV:
30233141-1 Nadmiarowa macierz niezależnych dysków (RAID)
32420000-3 Urządzenia sieciowe
48710000-8 - Pakiety oprogramowania do kopii zapasowych i odzyskiwania

- **Deduplikator wraz z wdrożeniem – 1 sztuka**

1. Minimalne parametry techniczne deduplikatora z funkcją ochrony przed Ransomware:
    1) Rozwiązanie musi być spójnym, dedykowanym urządzeniem przeznaczonym do przechowywania danych kopii zapasowych (appliance). Całość zaoferowanego rozwiązania musi pochodzić od tego samego producenta – nie dopuszcza się integrowania urządzeń i oprogramowania różnych producentów w celu realizacji poniższych wymagań.
    2) Rozwiązanie musi być obecne na rynku i dostępne w autoryzowanym kanale sprzedaży producenta od minimum pięciu lat. **Zamawiający będzie wymagał przed podpisaniem umowy na realizację zamówienia aby wykonawca, którego oferta została wybrana, dostarczył oświadczenie producenta potwierdzające pochodzenie sprzętu z oficjalnego kanału dystrybucji wraz z oświadczeniem o spełnieniu wymogów minimum 36 miesięcznej gwarancji.** Nie dopuszcza się prototypów.
    3) Rozwiązanie musi mieć możliwość instalacji w standardowej szafie rack 19”. Wraz z urządzeniami składającymi się na rozwiązanie należy dostarczyć komplet kabli (zasilających, sieciowych itp.).
    4) Rozwiązanie musi umożliwiać optymalizację składowania długoterminowego poprzez efektywne mechanizmy kompresji i/lub deduplikacji danych. Realizacja tego wymagania może być wykonywana inline, adaptacyjnie bądź jako proces działający w tle, pod warunkiem spełnienia opisywanych wymagań pojemnościowych i wydajnościowych.
    5) Rozwiązanie musi udostępniać zasoby do systemu kopii zapasowych z wykorzystaniem minimum protokołów CIFS i NFS.
    6) Rozwiązanie musi pozwalać na udostępnienie zasobów do różnych aplikacji do wykonywania kopii zapasowych. Jeżeli konkretne wymaganie nie stanowi inaczej (tj. nie wskazuje konkretnej funkcji aplikacji używanej przez zamawiającego), poniższe wymagania muszą być realizowane dla dowolnej aplikacji do wykonywania kopii zapasowych.
    7) Rozwiązanie musi być wyposażone w minimum 2 interfejsy 1 GbE ze złączem RJ-45 oraz minimum 2 interfejsy 10 GbE SFP+ z wkładkami 10GBASE-SR.
    8) Rozwiązanie musi umożliwiać zapis danych protokołem obiektowym, natywnie wspieranym przez oprogramowanie Veeam Backup and Replication (SOSAPI).

Potwierdzeniem tego wsparcia musi być informacja w bazie danych producenta oprogramowania, dostępnej na stronie https://www.veeam.com/partners/alliance-partner-technical-programs.html

9) Architektura rozwiązania musi uwzględniać wysoką dostępność i obejmować co najmniej:
   a. dyski wymienne w trakcie pracy urządzenia,
   b. redundantne zasilacze wymienne w trakcie pracy urządzenia,
   c. dyski w konfiguracji RAID-6 z zapasowym dyskiem "hot-spare",
   d. redundantne wentylatory.
10) Pojemność rozwiązania musi umożliwiać wykonywanie kopii zapasowej 25TB danych źródłowych, których kopie zapasowe będą przechowywane z następującą retencją: kopie dzienne przez okres 14 dni, pełne kopie tygodniowe przez okres 8 tygodni, pełne kopie miesięczne przez okres 12 miesięcy oraz pełne kopie roczne przez okres 3 lat.
11) Dla wybranych zestawów chronionych danych, rozwiązanie musi umożliwiać wykonywanie zadań backupu pełnego i nie mniej niż 60 kopii przyrostowych do wykonania kolejnego backupu pełnego bądź syntetycznego.
12) Zakładany roczny przyrost ilości danych źródłowych to 2-5%. Przyrost należy uwzględnić w doborze pojemności rozwiązania.
13) Niezależnie od powyższego, minimalna dostarczana pojemność użytkowa (po skonfigurowaniu odpowiedniej nadmiarowości) dysków nie może być niższa niż 50TB.
14) Jeżeli dostarczona pojemność użytkowa nie będzie wystarczająca do przechowywania danych źródłowych z retencją opisaną w punkcie 10), wykonawca będzie zobowiązany do dostarczenia rozbudowy pojemności na swój koszt w taki sposób, żeby umożliwić zrealizowanie zadanej retencji dla właściwych kopii zapasowych.
15) Rozwiązanie musi współpracować (być oficjalnie wspierane) z oprogramowaniem do ochrony danych Veeam Backup & Replication. Za rozwiązanie oficjalnie wspierane uważa się rozwiązanie opisane na stronie producenta pod adresem https://helpcenter.veeam.com/docs/backup/vsphere/deduplicating_storage_appliances.html?ver=120.
16) Dla zwiększenia wydajności i bezpieczeństwa, rozwiązanie musi umożliwiać wymianę danych z użytkowanym przez zamawiającego oprogramowaniem Veeam Backup & Replication poprzez natywny dla tego oprogramowania komponent Veeam Accelerated Data Mover uruchomiony bezpośrednio na systemie operacyjnym dostarczanego urządzenia do przechowywania danych kopii zapasowej, bez potrzeby stosowania dodatkowych, zewnętrznych urządzeń typu brama (Gateway Server).
17) Rozwiązanie musi umożliwiać rozbudowę do pojemności użytecznej min. 300 TB bez konieczności wymiany żadnych istniejących komponentów.
18) Rozwiązanie powinno automatycznie przechowywać najnowszy, pełny backup w formie niezdeduplikowanej gotowej do natychmiastowego odtworzenia, zgodnie z zaleceniem Veeam (artykuł techniczny Veeam KB2660 - https://www.veeam.com/kb2660)
19) Rozwiązanie musi mieć możliwość skalowalnej liniowo rozbudowy w zakresie jednocześnie pojemności i wydajności (architektura scale-out), tj. zapewniać stałą długość okna backupowego wraz z rosnącą ilością danych przechowywanych w ramach pojedynczej puli deduplikacyjnej w każdej lokalizacji. Realizacja tego wymagania nie może

być dokonywana poprzez rozbudowę jedynie dysków/półek dyskowych (architektura scale-up).

20) Producent musi gwarantować niezmienność ceny na rozbudowę rozwiązania o kolejne urządzenie wchodzące w skład oferowanej konfiguracji w cenie nie wyższej niż koszt pojedynczego urządzenia dostarczanego inicjalnie. Gwarancja taka musi obowiązywać minimum przez cały okres trwania wsparcia producenta, opisanego w punkcie 32).
21) Producent urządzeń wchodzących w skład rozwiązania musi pisemnie gwarantować, iż oferowane urządzenia nie zostaną objęte klauzulą zakończenia wsparcia (End-of-support) w okresie minimum 7 lat od podpisania przez zamawiającego protokołu odbioru zamówienia. W przypadku objęcia w tym czasie dostarczonych urządzeń powyższą klauzulą, wykonawca zobowiązany będzie do wymiany dostarczonych urządzeń na nowsze, nie objęte taką klauzulą wraz z przeprowadzeniem całkowitej migracji przechowywanych danych na własny koszt.
22) Całkowita przepustowość urządzenia podczas tworzenia kopii zapasowych i odzyskiwania danych musi wynosić nie mniej niż 6 TB/h. Przepustowość ta musi być potwierdzona dokumentacją producenta. Osiągnięcie wymaganej przepustowości nie może powodować obciążenia systemu chronionego, a jedynie być wewnętrzną przepustowością urządzenia - tj. nie może uwzględniać autorskich mechanizmów optymalizacji danych mających wpływ na wydajność systemu chronionego lub serwera backupu.
23) Jeżeli jakakolwiek z opisywanych w niniejszym dokumencie funkcjonalności wymaga dostarczenia licencji na pojedyncze urządzenie, pojedynczy kontroler, półkę dyskową bądź licencji pojemnościowej, należy dostarczyć je na całkowitą dostarczaną pojemność rozwiązania.
24) Rozwiązanie musi oferować możliwość wykonywania replikacji do/z posiadanego przez zamawiającego urządzenia tego samego producenta w innej jednostce, przetwarzania danych. Transfer danych do innej jednostki musi się odbywać się przez sieć WAN w taki sposób, aby minimalizować wykorzystanie przepustowości łącza (wysyłanie wyłącznie zmienionych bloków). Jeśli do replikacji wymagana jest licencja, należy dostarczyć ją na całkowitą dostarczaną pojemność rozwiązania dla urządzenia źródłowego i docelowego.
25) Rozwiązanie musi obsługiwać logowanie do konsoli przy użyciu uwierzytelniania dwuskładnikowego (2FA), które polega na integracji poświadczeń użytkownika z generatorem jednorazowych haseł opartych o sygnaturę czasu (TOTP).
26) Rozwiązanie musi umożliwiać przyznawanie użytkownikom ról o różnych poziomach uprawnień (Role-based Access Control), w tym co najmniej użytkownika (tylko prawa do przeglądania), operatora (prawa do nieniszczących zmian) i administratora (z najszerszym zakresem uprawnień).
27) Wymagane jest, aby role można było skonfigurować w taki sposób, aby żaden użytkownik, niezależnie od poziomu uprawnień, nie mógł samodzielnie zmienić lub wyłączyć ochrony przed skutkami oprogramowania ransomware, o którym mowa w punkcie 29), ani spowodować innych uszkodzeń danych, takich jak usunięcie udostępnionego zasobu wraz z jego zawartością.

28) Rozwiązanie musi być w stanie wykryć i powiadomić administratora o potencjalnych niepożądanych działaniach w ramach udostępnionych udziałów, takich jak usunięcie znacznej ilości danych lub zaszyfrowanie danych.
29) Rozwiązanie musi posiadać zintegrowany mechanizm "antyransomware", umożliwiający odzyskanie danych zaszyfrowanych/uszkodzonych/usuniętych przez ransomware, błąd ludzki lub celowe działanie.
30) Mechanizm "antyransomware" nie może negatywnie wpływać na działanie oprogramowania do backupu, w szczególności nie może blokować możliwości zapisu/modyfikacji istniejących plików backupu (np. jak mechanizm WORM - write once, read many).
31) Mechanizm "antyransomware" musi umożliwiać odtworzenie stanu zasobów urządzenia do wybranego punktu w czasie z okresu nie krótszego niż 30 dni wstecz, z możliwością konfiguracji tego okresu od 1 do 30 dni.
32) Urządzenie musi być objęte serwisem producenta świadczonym w trybie 8x5xNBD przez okres minimum 3 lat.
33) Wsparcie producenta musi gwarantować zamawiającemu konkretnego, dedykowanego inżyniera wsparcia poziomu L2 przez cały okres trwania wsparcia. Bezpośrednie informacje kontaktowe do dedykowanego inżyniera (numer telefonu, adres email) umożliwiające uzyskanie wsparcia muszą być dostępne dla zamawiającego i uaktualniane na bieżąco w razie jego zmiany.

2. W ramach prac zamawiający wymaga od wykonawcy:
   1) Wykonanie projektu wdrożenia uwzględniającego umieszczenie systemu w infrastrukturze zamawiającego.
   2) Instalację komponentów wraz z uruchomieniem systemu zgodnie z zatwierdzonym przez zamawiającego projektem.
   3) Przeprowadzenie testów odtworzeniowych dla wybranej próbki danych.
   4) Wykonanie dokumentacji powdrożeniowej.
   5) Przeprowadzenie szkolenia stanowiskowego z obsługi w/w rozwiązania w siedzibie zamawiającego dla dwóch administratorów.

➢ **Program do systemu backupu wspierający protokół natywny – 1 szt.**

1. Wymagania ogólne

Zamawiający wymaga kompletu licencji w wersji wieczystej, umożliwiających zabezpieczenie co najmniej 10 maszyn wirtualnych

1) Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5.
2) Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności

w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.

3) Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
4) Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej.
5) Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków.
6) Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
7) Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
8) Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.
9) Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.
10) Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.
11) Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania.
12) Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time).
13) Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu.
14) Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API.
15) Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.
16) Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji.

17) Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania.
18) Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
19) Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej
20) Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np.: skasowanie backupu, dodanie kolejnego administratora).
21) Oprogramowanie musi posiadać integracje z systemami zarządzania kluczami szyfrującymi (KMS).
22) Oprogramowanie musi posiadać integracje z systemami typu SIEM.
23) Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji.

2. Wymagania RPO

1) Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej.
2) Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
3) Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru.
4) Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.
5) Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
6) Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz ActiData FlexStor II).
7) Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son).
8) Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.
9) Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
10) Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.

11) Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
12) Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.
13) Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik.
14) Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding).
15) Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN).

3. Wymagania RTO

1) Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
2) Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).
3) Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami.
4) Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre.
5) Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.
6) Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków.
7) Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.
8) Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików.
9) Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.

10) Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell.
11) Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM.
12) Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
13) Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł.
14) Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.
15) Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.
16) Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.
17) Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
18) Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.
19) Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji.
20) Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN.
21) Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle.
22) Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI.
23) Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2.
24) Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN.

4. Ograniczenie ryzyka

1) Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).

2) Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
3) Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem.
4) Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
5) Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malwa re.
6) Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania.
7) Oprogramowanie, bazując na wyuczonynym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków.
8) Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

5. Środowiska fizyczne

1) Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego.
2) Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych.
3) Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE
4) Rozwiązanie musi wspierać system operacyjny macOS.
5) Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix.
6) Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą).
7) Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster.
8) Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów.
9) Rozwiązanie musi wspierać backup podłączonych dysków USB.
10) Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym.

11) Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury).
12) Rozwiązanie musi wspierać deduplikację oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone .
13) Rozwiązanie musi wspierać kontrolę pasma sieciowego.
14) Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych.
15) Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN.
16) Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft.
17) Rozwiązanie musi wspierać technologię BitLocker.
18) Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania.
19) Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych.
20) Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych.
21) Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle I PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu.
22) Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.
23) Rozwiązanie musi wspierać szyfrowanie.
24) Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne.
25) Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego.
26) Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej.
27) Rozwiązanie musi wspierać tworzenie wielu zadań backupowych.

6. Monitoring

1) System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich.

2) System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie.
3) System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
4) System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter.
5) System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn.
6) System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel.
7) System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk.
8) System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora.
9) System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów.
10) System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard).
11) System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna.
12) System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego.
13) System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta.
14) System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
15) System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.
16) System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware.
17) System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.4

7. Raportowanie

1) System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie.

2) System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
3) System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
4) System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
5) System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF.
6) System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc.
7) System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach.
8) System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów.
9) System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych.
10) System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych.
11) System musi mieć możliwość analizowania „przeszacowanych" wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury.
12) System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta.
13) System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
14) System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach 'what-if'.
15) System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware.
16) System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots).
17) System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie.

- **Dyski SSD do macierzy dyskowej NetApp E5760 wraz z półką dyskową**

Minimalne wymagania komponentów do rozbudowy posiadanej przez zamawiającego macierzy dyskowej o dodatkową przestrzeń:

1. Zamawiający wymaga dostarczenia 10 szt. dysków twardych typu - Solid State Drive, min 800GB,12Gb,Non-FDE lub dysk równoważny spełniający poniższe wymagania:

1) dysk fabrycznie nowy w oryginalnym fabrycznym opakowaniu,
2) parametry techniczne w zakresie wydajności i pojemności minimum takie jak w przypadku dysku SSD, min 800GB,12Gb,Non-FDE,DE460C part numer E-X4086B-AD-C
3) pełna zgodność sprzętowa i programowa z macierzą NetApp E5760 posiadaną przez zamawiającego,
4) zainstalowanie dysku w macierzy nie może powodować ograniczenia czy utraty wsparcia technicznego NetApp dla macierzy,
5) zainstalowanie dysku w macierzy nie może powodować naruszenia licencji na oprogramowanie wbudowane kontrolerów macierzy firmy NetApp posiadanej przez zamawiającego,
6) gwarancja – dysk będzie objęty gwarancją NetApp zgodnie z warunkami producenta dla systemu macierzowego.
7) Zamawiający posiada macierz NetApp E5760 o numerze seryjnym: 952132000108
8) W ramach działań związanych z rozszerzeniem przestrzeni dyskowych posiadanej macierzy należy:
   1) dostarczyć i zainstalować dyski w macierzy,
   2) zweryfikować istniejący podział przestrzeni,
   3) dołożyć dyski do odpowiednich wolumenów,
   4) zweryfikować istniejące LUNy i ich zapotrzebowanie na przestrzeń oraz ewentualnie je rozszerzyć, zgodnie z zapotrzebowaniem,
   5) przeprowadzić testy, sporządzić dokumentację powykonawczą.

2. Do dostarczonych dysków SSD do posiadanej macierzy NetApp E5760 zamawiający wymaga dostarczenia i zainstalowania półki rozszerzającej 24 dyski wraz z niezbędnym okablowaniem.
3. Zamawiający będzie wymagał przed podpisaniem umowy na realizację zamówienia aby wykonawca, którego oferta została wybrana, dostarczył oświadczenie producenta potwierdzające pochodzenie sprzętu z oficjalnego kanału dystrybucji wraz z oświadczeniem o rozbudowie nie powodującej utraty gwarancji.

- **Przełączniki sieciowe 10 GbE – 2 sztuki**

Minimalne wymagania przełączników sieciowych (2 sztuki):

1. Ilość slotów Modułu SFP+:minimum 24
2. Ilość portów SFP28:minimum 4
3. Port konsoli RJ 45
4. Liczba portów USB 2.0:minimum 2
5. Typ przełącznika: Zarządzany L3
6. Wielkość tabeli adresów: 15000
7. Przepustowość rutowania/przełączania: minimum 650 Gbit/s
8. Pamięci bufora pakietów: minimum 32 MB
9. Wielkość pamięci Flash: minimum 512 MB
10. Maksymalne Latency (10 Gbps) 0,65 µs

11. Standardy komunikacyjne: IEEE 802.1D, IEEE 802.1Q, IEEE 802.1Qav, IEEE 802.1s, IEEE 802.1w, IEEE 802.1x, IEEE 802.3, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3ak, IEEE 802.3bz, IEEE 802.3u
12. Protokoły: OSPF, OSPFv2, OSPFv3, RIP, RIP-1, RIP-2
13. Maksymalna rozmiary: 1U, 19”
14. Przełącznik stackowalny
15. Pobór mocy: max. 120W
16. Gwarancja: min. 36 miesięcy
17. Zamawiający wymaga dostarczenia min. 18 szt. wkładek SFP+ 10G oraz kompatybilnych kabli o długości 5mb umożliwiających podłączenie systemu.

Część II zamówienia:

KOD CPV:
30233141-1 Nadmiarowa macierz niezależnych dysków (RAID)

Dostawa **i zainstalowanie dysków twardych SAS do macierzy dyskowej IBM FlashSystem 5000, będącej w posiadaniu Zamawiającego**.

1. Wymagane parametry techniczne
   Dysk twardy SAS (Serial Attached SCSI) do macierzy IBM FlashSystem 5000 lub dysk równoważny o parametrach technicznych nie gorszych niż:
   1) ilość: 18 sztuk,
   2) dysk twardy: SAS o pojemności minimum 1,8 TB,
   3) dysk fabrycznie nowy w oryginalnym, fabrycznym opakowaniu,
   4) parametry techniczne w zakresie wydajności i pojemności minimum: 1,8TB, 12Gb, 10 000 rpm, 2.5 cala, FRU 02PX589,
   5) pełna zgodność sprzętowa i programowa z macierzą IBM FlashSystem 5000 posiadaną przez zamawiającego,
   6) zainstalowanie dysku w macierzy nie może powodować ograniczenia czy utraty wsparcia technicznego IBM dla macierzy,
   7) zainstalowanie dysku w macierzy nie może powodować naruszenia licencji na oprogramowanie wbudowane kontrolerów macierzy firmy IBM posiadanej przez zamawiającego,
   8) gwarancja – dysk będzie objęty gwarancją IBM (producenta sprzętu) zgodnie z warunkami producenta dla systemu macierzowego,
   9) w przypadku uszkodzenia dysk pozostaje u zamawiającego i nie podlega wymianie gwarancyjnej, w razie potrzeby serwis ma możliwość weryfikacji uszkodzenia w siedzibie zamawiającego,
   10) Zamawiający posiada macierz IBM FlashSystem 5000 o numerze seryjnym: 781TL08 wraz z półką dyskową o numerze seryjnym: 781TP67.

Wymagania dotyczące instalacji dysków

W ramach działań związanych z rozszerzeniem przestrzeni dyskowych posiadanej macierzy należy:

1) dostarczyć i zainstalować dyski w macierzy,
2) zweryfikować istniejący podział przestrzeni,
3) dołożyć dyski do odpowiednich wolumenów,
4) zweryfikować istniejące LUNy i ich zapotrzebowanie na przestrzeń oraz ewentualnie je rozszerzyć, zgodnie z zapotrzebowaniem,
5) przeprowadzić testy,
6) sporządzić dokumentację powykonawczą.