**Opis przedmiotu zamówienia**

Przedmiotem Zamówienia jest dostarczenie systemu kopii bezpieczeństwa w celu podniesienia poziomu bezpieczeństwa teleinformatycznego.

**Stan obecny**

Zamawiający zarządza obecnie różnorodnymi systemami operacyjnymi, systemam HIS, ERP, bazami danych i aplikacjami, do których dostęp za pośrednictwem sieci teleinformatycznej zapewniony jest w trzech lokalizacjach tj. szpital w Poznaniu, szpital w Ludwikowie, szpital w Chodzieży. Głównym miejscem przetwarzania i przechowywania danych jest ośrodek mieszczący się w szpitalu w Poznaniu.

**Zamawiający w ramach przedmiotu zamówienia wymaga :**

Dostarczenie urządzeń, licencji oraz konfiguracja urządzeń i oprogramowania w celu wdrożenia systemu kopii bezpieczeństwa. W szczególności:

# Serwera backup-u dla lokalizacji szpital Poznań szt. 1

Serwer o następujących parametrach:

## Obudowa

1. Typu RACK, wysokość 2U;
2. Szyny umożliwiające wysunięcie serwera z szafy stelażowej wraz z ramieniem porządkującym kable z tyłu obudowy;
3. Możliwość zainstalowania min. 12 dysków twardych hot plug 3,5”;
4. Możliwość zainstalowania fizycznego zabezpieczenia (np. na klucz lub elektrozamek) uniemożliwiającego fizyczny dostęp do dysków twardych;
5. Zainstalowane min. 4 szt. dysków SSD SATA 1,92TB DWPD>2,5  Hot-Plug;
6. Zainstalowane min. 8 szt. dysków SAS lub NL-SAS 14TB  Hot-Plug;

## Płyta główna

1. Dwuprocesorowa;
2. Wyprodukowana i zaprojektowana przez producenta serwera;
3. Możliwość instalacji procesorów 38-rdzeniowych;
4. Zainstalowany moduł TPM 2.0;
5. Min. 7 złącz PCI Express generacji 4 w tym:
	* min. 4 fizyczne złącza o prędkości x16;
	* min. 3 fizyczne złącza o prędkości x8;
	* Opcjonalnie możliwość uzyskania 2 złącz typu pełnej wysokości;
	* Opcjonalnie możliwość uzyskania 8 aktywnych złącz PCI-e;
6. Min. 32 gniazda pamięci RAM;
7. Obsługa min. 4 TB pamięci RAM DDR4;
8. Obsługa min. 10 TB pamięci operacyjnej w konfiguracji RAM DDR4 + pamięć nieulotna;
9. Wsparcie dla technologii:
	* Memory Scrubbing;
	* SDDC;
	* ECC;
	* Memory Mirroring;
	* ADDDC;
10. Obsługa pamięci nieulotnej instalowanej w gniazdach pamięci RAM (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci);
11. Min. 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express)  nie zajmujące klatek dla dysków hot-plug.

## Procesory

1. Min. jeden procesor 16-rdzeniowy, taktowanie bazowe 2,4 GHz, architektura x86\_64;
2. osiągające w teście PASSMark wynik CPU Mark 29,000 pkt  (wynik osiągnięty dla jednego procesora). Wynik opublikowany na stronie https://www.cpubenchmark.net/cpu\_list.php

## Pamięć RAM

1. Min. 128 GB pamięci RAM;
2. DDR4 Registered min. 3200Mhz.

## Kontrolery LAN

1. Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express:
	* Min. 4x 10Gbit SFP+;
	* Możliwość uzyskania dwóch interfejsów 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;
2. Interfejsy LAN zainstalowane w slotach PCI-e:
	* Min. 4x 1Gbit Base-T.

## Kontrolery I/O

1. Kontroler SAS RAID dla dysków wewnętrznych posiadający 4GB pamięci cache, obsługujący poziomy RAID: 0,1,10,5,50,6,60 z podtrzymaniem pamięci cache w przypadku utraty zasilania;
2. Dwuportowy zewnętrzny kontroler HBA SAS 12G.

## Porty

1. Zintegrowana karta graficzna ze złączem VGA z tyłu serwera;
2. Min. 2 porty USB 3.0 wewnętrzne;
3. Min. 2 porty USB 3.0 dostępne z tyłu serwera;
4. Min. 2 porty USB 3.0 na panelu przednim;
5. Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem;
6. Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.

## Zasilanie, chłodzenie

1. Redundantne zasilacze hotplug o sprawności min. 96% (tzw. klasa Titanium) o mocy min. 900W;
2. Redundantne wentylatory hotplug.

## Zarządzanie

1. Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii następujących komponentów:
	* karty rozszerzeń zainstalowane w dowolnym  slocie PCI Express;
	* procesory CPU;
	* pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM;
	* wbudowany na płycie głównej nośnik pamięci M.2 SSD;
	* status karty zarządzającej serwera;
	* wentylatory;
	* bateria podtrzymująca ustawienia BIOS płyty głównej;
	* zasilacze;
	* system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym);
2. Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:
	* Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;
	* Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;
	* Dostęp poprzez przeglądarkę Web, SSH;
	* Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;
	* Zarządzanie alarmami (zdarzenia poprzez SNMP);
	* Możliwość przejęcia konsoli tekstowej;
	* Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM);
	* Obsługa serwerów proxy (autentykacja);
	* Obsługa VLAN;
	* Możliwość konfiguracji parametru Max. Transmission Unit (MTU);
	* Wsparcie dla protokołu SSDP;
	* Obsługa protokołów TLS 1.2, SSL v3;
	* Obsługa protokołu LDAP;
	* Integracja z HP SIM;
	* Synchronizacja czasu poprzez protokół NTP;
	* Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej;
3. Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);
4. Dedykowana, do wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash o pojemności min. 16 GB;
5. Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;
6. Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.

## Wspierane OS

1. Microsoft Windows Server 2022, 2019, 2016;
2. VMWare vSphere 6.7, 7.0;
3. Suse Linux Enterprise Server 15;
4. Red Hat Enterprise Linux 7.9, 8.3;
5. Hyper-V Server 2016, 2019.

## System operacyjny serwera backupu

Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy:

1. Możliwość wykorzystania min. 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania min. 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania  7000 maszyn wirtualnych.
4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
	* pozwalają na zmianę rozmiaru w czasie pracy systemu,
	* umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
	* umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
	* umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
	* Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
	* Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18. Mechanizmy logowania w oparciu o:
	* Login i hasło,
	* Karty z certyfikatami (smartcard),
	* Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..
20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
	* Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
	* Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach
	* Zdalna dystrybucja oprogramowania na stacje robocze.
	* Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej.
	* Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego).
	* Szyfrowanie plików i folderów.
	* Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
	* Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
	* Serwis udostępniania stron WWW.
	* Wsparcie dla protokołu IP w wersji 6 (IPv6),
	* Wsparcie dla algorytmów Suite B (RFC 4869),
	* Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
	* Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.
26. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

## Gwarancja

1. Min. 3 lata gwarancji producenta serwera w trybie on-site z gwarantowaną skuteczną naprawą w miejscu użytkowania sprzętu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Dyski twarde nie podlegają zwrotowi organizacji serwisowej;
2. Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu;
3. Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie;
4. Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty).

## Dokumentacja, inne

1. Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta;
2. Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE
3. Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki;
4. W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;
5. Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;
6. Należy dostarczyć i wstępnie skonfigurować system zarządzania infrastrukturą IT. Musi być możliwość monitorowania stanu środowiska IT minimum dla oferowanego serwera oraz biblioteki taśmowej. System zarządzania posiada jeden spójny interfejs GUI HTML do zarządzania całym oferowanym środowiskiem sprzętowym. System zarządzania opiera się o tzw. Virtual Appliance kompatybilny z platformą wirtualną VMware vSphere, Microsoft Hyper-V, KVM. System zarządzania umożliwia aktualizację oprogramowanie systemowego (firmware) na serwerach w zakresie wszystkich istotnych elementów sprzętowych min: BIOS, kontrolery RAID, kontrolery KVM, karty sieciowe. System zarządzania posiada wsparcie dla następujących mechanizmów komunikacji zewnętrznej: HTTPS, SNMP, IPMI. System zarządzania musi mieć możliwość wyeksportowania inwentarza środowiska co najmniej w postaci pliku CSV.
7. Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia

# Macierz dyskowa dla lokalizacji szpital Poznań szt. 1

System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19” z zajętością maks. 2U w tej szafie. Każdy skonfigurowany moduł/obudowa musi posiadać układ nadmiarowy zasilania i chłodzenia, zapewniający bezprzewodową pracę macierzy bez ograniczeń czasowych w przypadku utraty redundancji w danym układzie (zasilania lub chłodzenia). Każdy moduł/obudowa powinien posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii. Rozbudowa o dodatkowe moduły dla obsługiwanych dysków powinna odbywać się wyłącznie poprzez zakup takich modułów, bez konieczności zakupu dodatkowych licencji lub specjalnego oprogramowania aktywującego proces rozbudowy lub musi być dostarczona licencja na dwukrotność dostarczanej pojemności. Dostarczana macierz musi umożliwiać takie podłączenie półek, aby awaria lub/i usunięcie jednej z półek nie powodowało utraty dostępu do danych znajdujących się na pozostałych modułach. Oferowana macierz musi obsługiwać min. 142 dyski wykonane w technologii hot-plug. Wszystkie zainstalowane dyski hot-plug, z wyłączeniem dysków SSD stosowanych jako rozszerzenie pamięci Cache kontrolerów, muszą być dostępne dla zapisu danych Użytkownika. Macierz musi umożliwiać rozbudowę i jednoczesne podłączenie i używanie modułów (tzw. „półek dyskowych”) w rozmiarze 2U pozwalająca umieścić do 24 dysków 2,5” typu hotplug dla dysków SAS i SSD oraz w rozmiarze 2U dla 12 dysków 3,5” typu hotplug NL-SAS i SSD. Wymaga się aby macierz umożliwiała jednoczesne podłączenie i użycie dowolnego rodzaju i kombinacji wyżej wymienionych półek dyskowych (tj. 2,5” + 3,5”).

## Pojemność macierzy:

Min. 12 szt. dysków twardych NL-SAS lub SSD-SAS o pojemności 10TB każdy;

## Kontrolery

1. Kontrolery macierzy muszą obsługiwać tryb pracy w układzie active-active lub mesh-active, macierz musi być dostarczona z zainstalowanymi 2 kontrolerami;
2. Każdy z kontrolerów macierzy musi posiadać po16GB pamięci podręcznej Cache – kontrolery muszą obsługiwać między sobą mechanizm lustrzanej kopii danych (cache mirror) przeznaczonych do zapisu;
3. Macierz musi obsługiwać rozbudowę pamięci podręcznej cache dla operacji odczytu o 800GB poprzez instalację dodatkowych modułów pamięci w kontrolerach lub wykorzystanie pojemności zainstalowanych dysków SSD,
4. W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci podręcznej Cache dla zapisów muszą być zabezpieczone metodą trwałego zapisu na dysk.
5. Kontrolery muszą posiadać możliwość ich wymiany bez konieczności wyłączania zasilania całego urządzenia;
6. Macierz musi obsługiwać wymianę kontrolera RAID bez utraty danych zapisanych na dyskach.
7. Każdy z kontrolerów RAID powinien posiadać dedykowany minimum 2 interfejsy RJ-45 Ethernet obsługujący połączenia z prędkością minimum 1Gb/s dla zdalnej  komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy.
8. Kontrolery macierzy muszą być oparte o procesor wykonany w technologii wielordzeniowej.
9. Kontrolery macierzy muszą obsługiwać do 70 grup dyskowych w całym rozwiązaniu, bez konieczności wymiany dostarczonych kontrolerów
10. Oferowana macierz musi mieć wyprowadzone 2 porty iSCSI 10Gb/s SFP+ MMF LC do dołączenia serwerów bezpośrednio lub do sieci san na każdy kontroler RAID.
11. Macierz musi umożliwiać dołożenie do każdego z kontrolerów portów do transmisji danych (bez konieczności usuwania istniejących):
	* Min. 2x SAS 12Gb/s
	* Min. 2x FC 32Gb/s,
12. Dołożenie portów jw. nie może powodować wymiany samych kontrolerów RAID w oferowanym rozwiązaniu a w przypadku konieczność licencjonowania tej funkcjonalności macierz ma być dostarczona z aktywną licencja na instalację i obsługę każdego z wymienionych protokołów transmisji danych
13. Macierz posiada obsługę operacji plikowych I/O w sieci NAS w obrębie zainstalowanych kontrolerów. Protokoły dostępu: CIFS, NFS. W przypadku obsługi protokołów CIFS i NFS wymagana jest funkcjonalność agregacji przepustowości dla interfejsów dedykowanych do obsługi tych protokołów. Obsługa protokołów CIFS i NFS musi odbywać się jednocześnie. – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy

## Poziomy RAID

Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID:

* + Raid-1
	+ Raid-10
	+ Raid-5
	+ Raid-50
	+ Raid-6

## Dyski

1. Oferowana macierz musi wspierać dyski hot-plug:
	* dyski elektroniczne SSD i mechaniczne HDD z interfejsami SAS12Gb/s
	* dyski mechaniczne HDD o prędkości obrotowej 7,2 krpm, 10 krpm,
2. Macierz musi obsługiwać mieszaną konfigurację dysków hot-plug SSD i HDD w rozmiarach 2,5” i 3,5” zainstalowanych w dowolnym module rozwiązania;
3. Wszystkie dyski wspierane przez oferowany model macierzy muszą być wykonane w technologii hot-plug i posiadać podwójne porty SAS obsługujące tryb pracy full-duplex
4. Macierz musi obsługiwać min. 140 dysków SAS SSD w całym rozwiązaniu, bez konieczności dokupowania/wymiany żadnych innych elementów sprzętowych czy licencyjnych innych niż same półki dyskowe wraz z dyskami;
5. Możliwość rozbudowy oferowanego modelu macierzy do 520 dysków bez migracji i przenoszenia danych - jedynie poprzez wymianę modułu kontrolerów macierzy (bez konieczności wymiany posiadanych dysków, półek dyskowych, bez konieczności przenoszenia danych/ istniejącej struktury grup dyskowych/LUN, jak również z zachowaniem istniejącej gwarancji producenta na półki dyskowe i dyski;
6. Macierz musi umożliwiać skonfigurowanie każdego zainstalowanego dysku hot-plug jako dysk hot-spare (dysk zapasowy) lub wirtualna przestrzeń zapasowa:
	* Macierz posiada możliwość konfiguracji dysku hot-spare dla zabezpieczenia dowolnej grupy dyskowej RAID
	* Macierz posiada możliwość konfiguracji dysku hot-spare dedykowanego dla zabezpieczenia tylko wybranej grupy dyskowej RAID
7. W przypadku awarii dysku fizycznego i wykorzystania wcześniej skonfigurowanego dysku zapasowego wymiana uszkodzonego dysku na sprawny nie może powodować powrotnego kopiowania danych z dysku hot-spare na wymieniony dysk (tzw. CopyBackLess) lub nie wymaga zwolnienia zapasowej przestrzeni wirtualnej.
8. Macierz musi pozwalać na zaszyfrowanie danych zapisanych na wszystkich obsługiwanych dyskach SSD-SAS, HDD-SAS oraz HDD NL-SAS minimum kluczem AES256-bit dla danych blokowych – jeżeli w tym celu niezbędne jest zakupienie dodatkowych licencji bądź komponentów sprzętowych to należy je dostarczyć wraz z macierzą.
9. Macierz musi umożliwiać zaszyfrowanie całej dostępnej powierzchni użytkowej minimum kluczem AES256-bit.

## Opcje programowe

1. Macierz musi być wyposażona w system umożliwiający wykonanie kopii migawkowych
2. Macierz musi umożliwiać zdefiniowanie min. 4000 woluminów (LUN)
3. Macierz powinna umożliwiać podłączenie logiczne z serwerami i stacjami poprzez 1000 ścieżek logicznych FC
4. Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego kontrolerów RAID i dysków bez konieczności wyłączania macierzy oraz bez konieczności wyłączania ścieżek logicznych FC/iSCSI dla podłączonych stacji/serwerów
5. Macierz musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacje: powiększanie grup dyskowych, zwiększanie rozmiaru woluminu, migrowanie woluminu na inną grupę dyskową
6. Macierz musi posiadać wsparcie dla systemów operacyjnych : Microsoft Windows Server 2012R2, 2016, 2019, SuSE Linux Enterprise Server, Red Hat Linux Enterprise Server, HP-UNIX, IBM AIX, SUN Solaris, Vmware Vsphere;
7. Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem) dla połączeń FC i iSCSI.
8. Macierz musi posiadać możliwość uruchamiania mechanizmów zdalnej replikacji danych, w trybie synchronicznym i asynchronicznym, po protokołach FC oraz iSCSI, bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji. Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy jako tzw. storage-based data replication. Replikacja danych musi być obsługiwana w połączeniu z każdą macierzą z tej samej rodziny urządzeń wspierającą obsługę zdalnej replikacji danych. – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy;
9. Macierz musi posiadać możliwość tworzenia lokalnych tj. w obrębie zasobów macierzy, pełnych kopii danych (tzw. klony danych), kopii przyrostowych oraz kopii lustrzanych (mirror) – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy;
10. Macierz musi obsługiwać mechanizm ochrony priorytetów obsługi wybranych zasobów – za taki mechanizm uznaje się funkcję typu ‘cache partitioning’ lub ‘storage partitioning’.
11. Macierz musi obsługiwać adresację IP v.4 i IP v.6
12. Wraz z macierzą należy dostarczyć oprogramowanie lub moduły programowe typu plug-in pozwalające na integracje macierzy w środowiskach Vmware w zakresie obsługi mechanizmów: Vmware VAAI, Vmware VVOL, Vmware MultiPath IO – z subskrypcją do bezpłatnej aktualizacji w całym okresie obowiązywania gwarancji
13. Macierz musi obsługiwać mechanizmy Thin Provisioning, czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy.
14. Macierz musi obsługiwać mechanizmy typu AST (Automated Storage Tiering) tj. automatycznego migrowania i realokacji bloków danych pomiędzy różnymi technologiami dyskowymi na podstawie analizy częstotliwości operacji I/O dla tych bloków oraz wg potrzeb wydajnościowych serwerów, środowisk i aplikacji korzystających z zasobów macierzy. Mechanizm AST musi być obsługiwany przy korzystaniu zarówno z trzech jak z dwóch dostarczonych technologii dyskowych: SSD, SAS, NL-SAS. Macierz musi pozwalać na definiowanie różnych polityk i zasad migrowania danych w obrębie tej samej macierzy. Mechanizm AST musi pozwalać na definiowanie okna czasowego dla zbierania pomiarów wydajności operacji I/O oraz okna czasowego dla migrowania danych wg ustalonych zasad i polityk – minimalny definiowany czas trwania w/w operacji (długość okna czasowego) nie może być dłuższy niż 4 godziny. Mechanizm AST musi pozwalać na wykluczanie wybranych godzin i dni z pomiarów wydajności operacji I/O. – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy
15. Mechanizm AST musi być obsługiwać funkcję Quality-of-Services pozwalająca na zagwarantowaniu wydajności dla wybranych zasobów macierzy (woluminów) mierzonej jako maksymalny czas opóźnień operacji I/O wykonywanych przez serwer/środowisko/aplikację. – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy
16. Macierz musi wspierać usługi VSS (Volume ShadowCopy Services) w systemach klasy Microsoft Windows Sever – wymagane jest dostarczenie niezbędnego oprogramowania / sterowników VSS pozwalających na obsługę VSS przy maksymalnej pojemności i liczbie dysków obsługiwanych przez oferowaną. W czasie trwania gwarancji wymaga się bezpłatnego dostępu do nowych wersji oprogramowania i sterowników
17. Macierz musi obsługiwać mechanizmy migracji danych w trybie online z innej macierzy tej klasy, z zachowaniem obsługi operacji I/O dla serwerów podłączonych do migrowanej macierzy tj. do migrowanych zasobów LUN
18. Macierz wspiera rozwiązania klasy ‘klastra macierzowego’ tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform software’owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych pomiędzy minimum 2 macierzami protokołami FC oraz iSCSI. Mechanizm klastra macierzowego musi być obsługiwany dla protokołów FC oraz iSCSI, zarówno w zakresie replikacji danych jak i w zakresie sposobu podłączenia serwerów do zasobów macierzy. Pod użytym pojęciem ‘wysoka dostępność zasobów dyskowych’ należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do macierzy (macierz podstawowa) w przypadku wystąpienia awarii logicznego połączenia z tą macierzy bądź awarii samej macierzą, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej. Funkcjonalność ‘klastra macierzowego’ musi pozwalać na automatyczne i ręczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. Automated/manual failover). – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy

## Zarządzanie

1. Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym systemu pamięci masowej
2. Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym.
3. Musi być możliwe zdalne zarządzanie macierzą z wykorzystaniem standardowej przeglądarki internetowej (np. Internet Explorer, Google Chrome, Mozilla Firefox) bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora
4. Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI

## Gwarancja i serwis

1. Całe rozwiązanie musi być objęte min. 36 miesięcznym okresem gwarancji z naprawą miejscu instalacji urządzenia i z gwarantowaną skuteczną naprawą do końca następnego dnia roboczego od dnia zgłoszenia awarii do organizacji serwisowej producenta macierzy. Uszkodzone dyski twarde nie podlegają zwrotowi organizacji serwisowej.
2. Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego.
3. Po zakończeniu okresu gwarancji musi być zapewniony przez producenta rozwiązania bezpłatny dostęp do aktualizacji oprogramowania wewnętrznego oferowanej macierzy oraz do kolejnych wersji oprogramowania zarządzającego w okresie minimum 2 lat.
4. System musi zapewniać możliwość samodzielnego i automatycznego powiadamiania producenta i administratorów Zamawiającego o usterkach za pomocą wiadomości wysyłanych poprzez szyfrowany protokół. Funkcjonalność musi pozwalać na automatyczne otwarcie zgłoszenia serwisowego w bazie serwisowej producenta macierzy zgodnie z wymaganym w specyfikacji poziomem SLA; Opcja ta musi być dostępna bezpłatnie w trakcie całego okresu gwarancji producenta macierzy.  Oferowana funkcjonalność musi również umożliwiać konfigurację i uruchomienie zdalnego dostępu do macierzy bezpośrednio przez Producenta.
5. Macierz musi pochodzić z oficjalnego kanału sprzedaży producenta w UE. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych
6. Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia
7. Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty);
8. Producent oferowanej macierzy musi posiadać dedykowaną, ogólnie dostępną stronę internetową, gdzie po wpisaniu numeru seryjnego macierzy można zweryfikować co najmniej: czas i poziom oferowanego serwisu gwarancyjnego producenta zarówno dla macierzy jak i dowolnej z półek dyskowych, datę zakończenia wsparcia gwarancyjnego, datę zakończenia wsparcia producenta dla oferowanego urządzenia – w formularzu ofertowym należy podać adres internetowy strony producenta macierzy,  gdzie można zweryfikować wymagane informacje;

# Biblioteka taśmowa dla lokalizacji szpital Poznań szt. 1

## Obudowa i zasilanie

1. Biblioteka taśmowa w obudowie RACK 3U
2. Redundantne zasilania, minimum 2 zasilacze

## Napęd

1. Typ napędu zainstalowanego napędu – LTO-8 SAS
2. Liczba zainstalowanych napędów – min. 2
3. Liczba obsługiwanych napędów – min. 42
4. Liczba obsługiwanych slotów – min. 560
5. Liczba dostarczonych aktywnych slotów – min. 20
6. Liczba slotów Import/Export - min. 2
7. Wbudowany skaner kodów paskowych na nośnikach LTO

## Funkcje i kompatybilność

1. Lokalne zarządzanie za pomocą panelu/pulpitu operatora
2. Obsługa standardu LTFS
3. Funkcja partycjonowania, możliwość utworzenia 2 wirtualnych bibliotek
4. Obsługa szyfrowania danych na nośniku LTO
5. Obsługa nośników LTO RW oraz LTO WORM
6. Gwarantowana kompatybilność odczytu taśm LTO-7
7. Gwarantowana kompatybilność zapisu taśm LTO-7
8. Interfejs zdalnego zarządzania - Ethernet 10/100Mb/s złącze RJ-45

## Inne

1. Zapis danych: min. 300 MB/s
2. Odczyt danych: min. 750 MB/s
3. Rozmiar bufora: min. 1000 MB
4. Min. 2 nośniki czyszczące LTO
5. Min. 20 nośników LTO-8 RW
6. Min. 2 kable SAS do podłączenia oferowanej biblioteki do serwera backup

## Gwarancja

1. Min. 36 miesięczny okres gwarancji
2. Realizowana w miejscu instalacji sprzętu, gwarantowane skuteczne zakończenie naprawy sprzętu do końca następnego dnia roboczego od zgłoszenia.

## Normy i standardy

1. Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia

# Oprogramowanie backupu

## Wymagania ogólne

1. Licencja na min. 25 systemów operacyjnych ze wsparciem na min. 3 lata.
2. Oprogramowanie musi współpracować z infrastrukturą Vmware vSphere oraz Microsoft Hyper-V. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.
3. Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
4. Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.
5. Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V
6. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
7. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
8. Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
9. Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental)
10. 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
11. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając stworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.
12. Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych.
13. 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.
14. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
15. Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
16. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time)
17. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
18. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
19. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
20. 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
21. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
22. Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
23. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.

## 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 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
3. Oprogramowanie musi oferować ten mechanizm z dokładnością do datastoru
4. Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
5. 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 i być dostępna dla następujących macierzy: HPE, Dell EMC, NetApp, Cisco, IBM, Lenovo, Fujitsu, Huawei, INFINIDAT, Pure Storage.
6. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
7. Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn
8. Oprogramowanie musi posiadać wsparcie dla NDMP
9. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
10. Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
11. Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
12. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
13. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
14. Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
15. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
16. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
17. Oprogramowanie musi posiadać takie same funkcjonalności replikacji dla Hyper-V
18. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
19. Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere
20. Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing)

## 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 oraz Hyper-V niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych.
2. Dodatkowo dla środowiska vSphere 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 umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
6. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.
7. Oprogramowanie musi umożliwić odtworzenie plików 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
8. Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
9. Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików:
	* Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
	* BSD: UFS, UFS2
	* Solaris: ZFS, UFS
	* Mac: HFS, HFS+
	* Windows: NTFS, FAT, FAT32, ReFS
	* Novell OES: NSS
10. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
11. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
12. Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD, Microsoft System Objects, certyfikaty CA oraz elementy AD Sites.
13. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),
14. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat
15. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze. Opcja odtworzenia elementów, witryn, uprawnień.
16. 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.
17. Oprogramowanie musi pozwalać na zaprezentowanie baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego
18. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
19. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA
20. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

## Inne funkcjonalności

1. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
2. 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
3. Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere
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 umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

## Dostawa, wdrożenie, wsparcie techniczne i szkolenie

1. Wymagane jest aby producent zapewniał wsparcie techniczne minimum przez: telefon, e-mail, czat na żywo oraz zdalne połączenie przez okres minimum 3lat
2. Instalacja oprogramowania na wskazanym serwerze.
3. Wykonawca przeprowadzi szkolenie administracyjne dla minimum 5 osób