|  |  |
| --- | --- |
| LP | Nazwa |
|  | Dostawa i wdrożenie kompleksowego systemu backupu, zabezpieczającego infrastrukturę teleinformatyczną Urzędu Marszałkowskiego Województwa Podlaskiego  |
|  | Szkolenie certyfikowane produktowe z wdrożonej technologii dla administratorów wdrożonego Systemu: 1. poziom podstawowy minimum 3 dni po 8 godzin z wdrożonego rozwiązania – minimum 3 osoby,
2. poziom zaawansowany minimum 3 dni po 8 godzin z wdrożonego rozwiązania – minimum 3 osoby
 |

**System – Oprogramowanie do tworzenia kopii zapasowych wraz z urządzeniami niezbędnymi do jego działania**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa wymogu** | **Wymagane minimalne parametry techniczne sprzętu** |
|  | Wymagania ogólne | * 1. Oprogramowanie backupu musi być klasy „enerprise” przeznaczone dla średnich i dużych firm, które mają rozbudowane i heterogeniczne środowisko informatyczne.
	2. Oprogramowanie backupu musi wspierać wdrożenia na sprzęcie fizycznym, infrastrukturze wirtualnej oraz w chmurze.
	3. System musi zostać dostarczony w postaci komercyjnej platformy
	4. System musi być uruchomiony na urządzeniach o parametrach rekomendowanych przez producenta oprogramowania
	5. Urządzenia wchodzące w skład Systemu muszą być fabrycznie nowe, aktualnie obecne w linii produktowej producenta i jednocześnie nie mogą znajdować się na liście „end-of-sale” oraz „end-of-support” producenta
	6. Urządzenia Systemu muszą pochodzić z autoryzowanego kanału sprzedaży/dystrybucji producenta
	7. System musi się składać z urządzeń fabrycznie nowych, nieużywanych i wolnych od wad fizycznych, w szczególności bez wad zmniejszających jego wartość lub użyteczność wynikającą z jego przeznaczenia
	8. System musi być wolny od wad prawnych, a w szczególności nie stanowić własności osoby trzeciej ani nie może być obciążony jakimkolwiek prawem przysługującym osobie trzeciej, które wyłącza lub ogranicza możliwość przeniesienia prawa własności Sprzętu na Zamawiającego
	9. System musi posiadać dołączone niezbędne instrukcje i materiały dotyczące użytkowania w języku polskim lub angielskim
	10. System musi posiadać trwałe oznaczenia zawierające: nazwę producenta, typ, oznakowanie CE, numer fabryczny (o ile są przewidziane przez producenta)
	11. System musi składać się z: oprogramowania backupu wraz z niezbędnymi licencjami, PBBA (Purpose Built Backup Appliance), biblioteki taśmowej, innych komponentów sprzętowych lub licencji oprogramowania niezbędnych do realizacji proponowanego rozwiązania i przedstawionych wymagań np. serwerów zarządzających, serwerów pośredniczących w backupie wirtualnych maszyn, serwerów do obsługi biblioteki taśmowej, systemów operacyjnych na dostarczone serwery itd. Nie jest dopuszczalne wykorzystanie w proponowanym rozwiązaniu infrastruktury serwerowej posiadanej aktualnie przez Zamawiającego.
	12. System jest kompatybilny i możliwy do wdrożenia w infrastrukturze teleinformatycznej Zamawiającego, a Wykonawca oświadcza, że zapoznał się z wykorzystywaną przez Zamawiającego technologią, w tym używanym sprzętem, oprogramowaniem, doprowadzonym zasilaniem, zabezpieczeniami, architekturą serwerową oraz sieciową, systemami operacyjnymi oraz że przedmiot umowy będzie prawidłowo funkcjonować w zakresie, w jakim to konieczne do realizacji przedmiotu umowy w kooperacji ze sprzętem i oprogramowaniem Zamawiającego przy uwzględnieniu zabezpieczeń wykorzystywanych przez Zamawiającego
	13. Wszystkie wymagania - o ile nie wskazano inaczej - muszą być spełnione przez jedno oprogramowanie backupu określone w dokumentacji technicznej producenta własną nazwą oraz wersją nawet w przypadku jeśli dostarczana licencja pozwala na stosowanie wielu różnych oprogramowań zawartych w jednym pakiecie licencyjnym.
 |
|  | Ogólne parametry fizyczne | * 1. Urządzenia muszą być dedykowany przez producenta do montażu w 19” szafie RACK Zamawiającego.
	2. Uszkodzenie urządzeń musi być raportowane na urządzeniu w formie wizualnej np. dioda, wyświetlacz LCD itp.
 |
|  | Zasilacze | * 1. Każde z urządzeń wchodzących w skład Systemu musi być wyposażone w minimum dwa zasilacze zapewniające redundancję zasilania w trybie hot-plug.
	2. Połowa zainstalowanych zasilaczy musi zapewnić zasilanie wyposażonego urządzenia, przy zachowaniu jego pełnych możliwości funkcjonalnych oraz wydajnościowych.
	3. Zasilacze muszą pracować z siecią energetyczną Zamawiającego o parametrach AC 230V, 50Hz.
 |
|  | Interfejsy | * 1. Ilość interfejsów w urządzeniu/ach powinna być taka żeby podłączyć dostarczane urządzenia do przełączników sieciowych o przepustowości 10GbE i/lub sieci danych FC 16Gb – przynajmniej do dwóch przełączników typu core. Wkładki światłowodowe preferowane do połączenie do przełączników - jednomodowe min. 10km.
	2. Posiadać odrębny/e niezbędny/e interfejs/y do połączenia dostarczanego urządzenia taśmowego umożliwiające przechowywanie danych na nośnikach taśmowych typu LTO.
	3. Każde dostarczone urządzenie będzie posiadało przynajmniej po jednym interfejsie do zarządzania nim niezależnym od interfejsu danych.
 |
|  | Zarządzanie | * 1. Oprogramowanie backupu musi posiadać scentralizowaną administrację - jedna konsola zarządzająca do pełnej administracji Systemem.
	2. Oprogramowanie backupu musi umożliwiać administrację za pomocą GUI (aplikacja lub web), CLI oraz RESTful API.
	3. Oprogramowanie backupu musi posiadać centralną konsolę zarządzania środowiskiem kopii zapasowych. Konsola musi umożliwiać:
1. monitorowanie i zarządzanie wszystkimi zadaniami wykonywania i odtwarzania kopii zapasowych, tworzenia duplikatów wykonanych kopii zapasowych,
2. ustawianie harmonogramów wykonywania kopii zapasowych,
3. monitorowanie i kontrolowanie urządzeń składowania kopii zapasowych podłączonych do serwerów nośników,
4. centralne zarządzanie konfiguracją, właściwych dla oprogramowania systemu ustawień serwera zarządzającego, serwera nośników, klientów,
5. odtwarzania kopii zapasowych.
	1. Oprogramowanie backupu musi posiadać obsługę z poziomu wiersza poleceń. Obsługa z poziomu wiersza poleceń musi umożliwiać:
6. konfigurację i modyfikację polityk wykonywania kopii zapasowych,
7. konfigurację i modyfikację harmonogramów wykonywania kopii zapasowych,
8. konfigurację i modyfikację urządzeń składowania kopii zapasowych podłączonych do serwerów nośników,
9. konfigurację i modyfikację nośników taśmowych,
10. monitorowanie i kontrolowanie zadań kopii zapasowych,
11. konfigurację i modyfikację nośników taśmowych,
12. konfigurację i modyfikację właściwych dla oprogramowania systemu, ustawień serwera zarządzającego, serwera nośników, klientów,
13. konfigurację, modyfikację i przeglądanie dzienników Serwera zarządzającego, serwera nośników, klientów.
	1. Oprogramowanie musi posiadać możliwość definiowania uprawnień dla administracji systemem w oparciu o role, a w szczególności definiowania użytkowników i grup z różnymi uprawnieniami np. operator backupu.
 |
|  | Architektura rozwiązania | * 1. Serwer zarządzający oprogramowania backupu musi być dostępny co najmniej na platformę Windows Server, 2019, 2022, RHEL 8, 9, SLES 12, 15 lub utwardzony Linux
	2. Serwer nośników oprogramowania backupu musi być dostępny co najmniej na platformę Windows, 2019, 2022, Oracle Linux 8, 9, RHEL 8, 9, SLES 12, 15 lub utwardzony Linux
	3. Klient oprogramowania backupu musi być dostępny co najmniej na platformę Windows Server 2012, 2012R2, 2016, 2019, 2022, Oracle Linux 8, 9, Solaris 10 i 11, RHEL 8, 9. SLES 12, 15, Debian 11, 12, Ubuntu od 16.
 |
|  | Baza katalogowa systemu backupu | * 1. Baza katalogowa oprogramowania backupu musi być częścią systemu backupu i być zainstalowana na serwerze zarządzającym.
	2. Baza katalogowa oprogramowania backupu nie może posiadać ograniczeń wynikających z ilości używanych w serwerze procesorów i rdzeni procesorów.
	3. Baza katalogowa oprogramowania backupu musi być w cenie systemu kopii zapasowych i nieograniczona co do ilości środowisk backupowych, mocy czy ilości serwerów czy to backupowych czy produkcyjnych. Jakakolwiek rozbudowa środowiska backupowego czy dodanie następnego nie może powodować konieczności dokupienia licencji dla tej bazy.
 |
|  | Disaster Recovery | * 1. System musi umożliwiać rozbudowę o drugie urządzenie deduplikujące i replikację kopii zapasowych pomiędzy lokalizacjami w postaci zdeduplikowanej tzn. przesyłane są tylko unikatowe/nieznane bloki danych w ośrodku docelowym. Zreplikowane kopie zapasowe muszą być automatycznie dostępne dla odtwarzania w ośrodku docelowym. Replikacja danych musi odbywać się bezpośrednio pomiędzy urządzeniami dyskowymi. Proces replikacji musi być całkowicie zarządzany z poziomu oprogramowania backupu.
	2. W przypadku awarii/niedostępności jednego z ośrodków objętych rozwiązaniem backupu oprogramowanie backupu musi umożliwiać szybkie uruchomienie systemu backupu w ośrodku działającym i umożliwienie odtwarzania z repliki kopii zapasowych bez wykonywania dodatkowych operacji np. importowania/skanowania nośników. Czas przywrócenia dostępności systemu backupu po awarii ośrodka nie może być dłuższy niż 10 minut. Dopuszczalne jest zastosowanie do tego celu oprogramowania klastrowego firmy trzeciej dla serwera zarządzającego.
 |
|  | Obsługa LAN/SAN | * 1. Oprogramowanie backupu musi umożliwiać backup przez sieć LAN serwerów fizycznych oraz wirtualnych z systemami Windows Server 2016, 2019, 2022, Oracle Linux 8, 9, Solaris 10 i 11, RHEL 7, 8, 9. SLES 12, 15, Debian 11, 12, Ubuntu od 16
	2. Oprogramowanie backupu musi umożliwiać backup przez sieć FC SAN serwerów fizycznych bezpośrednio na oferowane urządzenie dyskowe z pominięciem jakichkolwiek serwerów pośredniczących lub inny mechanizm zapewniający wykonywanie kopii zapasowej w sposób nieobciążający serwerów produkcyjnych zamawiającego. W celu realizacji tej funkcjonalności dopuszczalne jest zainstalowanie na serwerach fizycznych tylko klienta oprogramowania backupu – nie jest dopuszczalne instalowanie serwera nośnika mediów. Funkcjonalność ta musi być dostępna dla klientów backupu z systemami operacyjnymi od minimum: Windows Server 2016 i nowsze, Linux RHEL 7 i nowsze, SLES 12 i nowsze.
	3. Oprogramowanie backupu będzie umożliwiać backup na bibliotekę taśmową poprzez FC SAN. Nie jest dopuszczalne instalowanie w tym celu serwerów typu nośnik mediów na zabezpieczanych systemach/klientach backupu. Jeżeli realizacja tej funkcjonalności wymaga instalacji nośnika mediów poza dostarczanym urządzeniem dyskowym należy dostarczyć dodatkowy serwer fizyczny na ten cel w konfiguracji zalecanej przez producenta umożliwiającej osiągnięcie pełnej wydajności oferowanej biblioteki taśmowe.
 |
|  | Backup urządzeń NAS | * 1. Oprogramowanie powinno umożliwiać backup macierzy dyskowych typu NAS z wykorzystaniem protokołu NDMP lub inny sposób zapewniający dużą wydajność przesłania danych. Nie jest dopuszczalne stosowanie do tego celu dodatkowych pośredniczących elementów.
	2. Oprogramowanie musi umożliwiać wykonywanie backupu NDMP lub w inny sposób zapewniający dużą wydajność przesłania danych przez sieć LAN bezpośrednio na dostarczone urządzenie dyskowe bez udziału jakichkolwiek serwerów pośredniczących.
	3. Oprogramowanie musi umożliwiać wykonywanie backupu NDMP bezpośrednio na bibliotekę taśmową fizyczną oraz wirtualną VTL podłączoną do macierzy dyskowej NAS za pośrednictwem sieci FC SAN z wyłączeniem jakichkolwiek serwerów pośredniczących, lub w inny sposób zapewniający dużą wydajność przesłania danych.
 |
|  | Deduplikacja | * 1. Oprogramowanie backupu musi posiadać własny wbudowany mechanizm globalnej deduplikacji w trybie inline lub integrować się w tym celu z dostarczonym urządzeniem deduplikującym. Przy czym integracja z urządzeniem deduplikującym musi odbywać się przez specjalistyczne API pozwalając na:
1. wykonywanie deduplikacji na klientach oprogramowania backupu (algorytmem urządzenia deduplikującego lub równoważny, gwarantujący szybkie wykonanie kopii zapasowej bez obciążania serwera produkcyjnego),
2. transfer danych bezpośrednio z klientów oprogramowania backupu do urządzenia deduplikującego zarówno przez sieć LAN jak i/lub FC SAN bez udziału jakichkolwiek serwerów pośredniczących,
3. wykonywanie wirtualnych kopii syntetycznych,
4. zarządzanie replikacją danych wykonywaną bezpośrednio pomiędzy urządzeniami deduplikującymi
	1. Musi istnieć możliwość wykonywania deduplikacji na kliencie backupu lub równoważny mechanizm, zapewniający nieprzerwaną pracę systemu w trakcie wykonywania kopii zapasowej. Nie jest dopuszczalne instalowanie w tym celu na backupowanym serwerze oprogramowania serwera nośników,
	2. Musi istnieć możliwość wykonywania deduplikacji na serwerze nośników.
	3. System musi umożliwiać wykonywanie deduplikacji z wykorzystaniem zmiennej długości bloku.
 |
|  | Przechowywanie danych | * 1. Oprogramowanie backupu musi obsługiwać biblioteki taśmowe, biblioteki wirtualne (VTL) oraz urządzenia deduplikujące. Przy czym integracja z urządzeniem deduplikującym musi odbywać się przez specjalistyczne API pozwalając na:
1. wykonywanie deduplikacji na klientach oprogramowania backupu (algorytmem urządzenia deduplikującego lub równoważny, gwarantujący szybkie wykonanie kopii zapasowej bez obciążania serwera produkcyjnego),
2. transfer danych bezpośrednio z klientów oprogramowania backupu do urządzenia deduplikującego zarówno przez sieć LAN jak i/lub FC SAN bez udziału jakichkolwiek serwerów pośredniczących,
3. wykonywanie wirtualnych kopii syntetycznych,
4. zarządzanie replikacją danych wykonywaną bezpośrednio pomiędzy urządzeniami deduplikującymi,
	1. System musi wspierać głównych dostawców chmur publicznych jako magazyn kopii zapasowych. Dane przesyłane i składowane w chmurze muszą być w formie zdeduplikowanej w celu optymalizacji wykorzystania łącz sieciowych oraz zasobów w chmurze.
	2. Oprogramowanie backupu musi posiadać możliwość wykonywania backupów na urządzenia dyskowe, które następnie będą automatycznie powielane na nośniki taśmowe (D2D2T) lub do chmury (D2D2TC). System musi, tak długo jak dane obecne są na dyskach, wykorzystywać je w procesach odtwarzania.
	3. Oprogramowanie backupu musi posiadać możliwość równoczesnego zapisu/odczytu na wielu napędach taśmowych w tym samym czasie.
	4. Oprogramowanie backupu musi automatyzować tworzenie wielu kopii zapasowych na różnych urządzeniach magazynowych z różną retencją przechowywania danych.
	5. Oprogramowanie backupu musi wspierać topologie replikacji danych typu jeden-do-jednego, wiele-do-jednego, jeden-do-wielu oraz kaskadową z wykorzystaniem deduplikacji danych w celu zminimalizowania ilości przesyłanych danych.
	6. Oprogramowanie backupu musi wspierać szyfrowanie danych.
	7. Oprogramowanie musi umożliwiać zarządzanie retencją kopii zapasowych w oparciu o kalendarz/czas przechowywania kopii zapasowych.
 |
|  | Źródła danych - ogólnie | * 1. Oprogramowanie backupu musi umożliwiać wykonywanie kopii zapasowych w środowisku heterogenicznym za pomocą, dedykowanego dla platformy systemowej, klienta systemu kopii zapasowych.
	2. Oprogramowanie backupu musi umożliwiać wykonywanie kopii pełnych, przyrostowych oraz syntetycznych w zależności od typu danych.
	3. Oprogramowanie backupu musi umożliwiać funkcjonalność load-balancingu dla serwerów nośników pozwalającą na dystrybuowanie ruchu zadań backupowych pomiędzy nimi.
	4. Oprogramowanie backupu musi umożliwiać wykonywanie skryptów przed i po backupie.
	5. Oprogramowanie backupu musi umożliwiać definiowanie kalendarzy automatycznego wykonywania kopii zapasowych
 |
|  | Źródła danych – systemy plików | * 1. Klient oprogramowania backupu musi umożliwiać backup systemów plików na platformach minimum: Windows Server 2012, 2012R2, 2016, 2019, 2022 i nowsze, Oracle Linux 8, 9, Solaris 10 i 11, RHEL 7, 8, 9. SLES 12, 15, CentOS 7, Debian 11, 12, Ubuntu od wersji 16.
	2. Dla systemów Windows Server oprogramowanie backupu musi wykorzystywać do backupu mechanizm VSS.
	3. Oprogramowanie backupu musi umożliwiać restartowanie zadań backupowych w przypadku ich awarii od miejsca (tzw. checkpoint restart), w którym nastąpiła awaria, a nie od początku zadania.
	4. Oprogramowanie backupu musi posiadać wbudowany mechanizm szyfrowania danych przesyłanych przez sieć LAN.
	5. Oprogramowanie backupu musi posiadać możliwość kompresji i deduplikacji na kliencie backupowym przed wysłaniem danych przez sieć lub równoważny zapewniający nieprzerwaną pracę serwerów produkcyjnych bez straty wydajności
	6. Oprogramowanie backupu musi posiadać funkcjonalność umożliwiającą wydajny backup milionów małych plików.
 |
|  | Źródła danych – bazy danych i aplikacje | * 1. Oprogramowanie backupu musi posiadać dedykowanego agenta instalowanego na zabezpieczanych serwerach i umożliwiającego spójny backup w trybie online oraz odtwarzanie następujących baz danych i aplikacji: MS Exchange 2016, 2019, MS Sharepoint 2016, 2019, MS SQL 2022, 2019, 2017, 2016, 2014 i 2012, MySQL 5, 8, Oracle 19c, 18c, 12c i 11g, PostgreSQL 9, 10, 11, 12, 13, 14, SAP HANA 1.0 SPS11, 1.0 SPS12, 2.0 SPS3, 2.0 SPS04, 2.0 SPS05, 2.0 SPS06.
	2. Backup baz danych i aplikacji musi być wykonywany poprzez integrację z API baz danych lub aplikacji Oracle RMAN, VSS, SQL VDI.
	3. Oprogramowanie backupu musi umożliwiać tworzenie polityk i terminarzy backupu baz danych Oracle z wykorzystaniem kreatora dostępnego z interfejsu graficznego (GUI).
	4. Oprogramowanie backupu musi automatycznie tworzyć skrypty do backupu baz Oracle (RMAN) na podstawie parametrów zapisanych w katalogu systemu backupu.
	5. Oprogramowanie backupu musi umożliwiać odtwarzanie Microsoft Active Directory na poziomie pojedynczych obiektów. Backup musi być realizowany wykonywany jednoprzebiegowo, a odtwarzanie całego AD i pojedynczych obiektów.
	6. Oprogramowanie backupu musi zapewniać wykonywanie kopii zapasowych i dzienników transakcji baz danych MS SQL, Oracle.
	7. Oprogramowanie backupu nie może wykorzystywać metody log-shipping do ochrony logów transakcyjnych baz MS SQL, Oracle.
	8. Oprogramowanie backupu musi wspierać pełne przywracanie i odzyskiwanie baz danych MS SQL, Oracle.
	9. Oprogramowanie backupu musi wspierać przywracanie logów transakcyjnych baz danych MS SQL, Oracle do określonego punktu w czasie.
 |
|  | Źródła danych – wirtualizacja | * 1. Oprogramowanie backupu musi wspierać minimalnie wersję VMware vSphere 6.5 i nowsze.
	2. Oprogramowanie backupu musi wspierać serwery vSphere zarządzane przez vCenter jak i samodzielne serwery ESXi od wersji 5.5
	3. Oprogramowanie backupu musi wspierać VMware vSAN 7.0, 8.0.
	4. Musi istnieć możliwość wykonywania backupu obrazów maszyn wirtualnych VMware vSphere z wykorzystaniem vStorage API for Data Protection oraz metod transmisji: NBD oraz HotAdd (w obu przypadkach transmisja przez sieć LAN) bez konieczności instalacji agenta wewnątrz tych maszyn.
	5. Oprogramowanie backupu musi umożliwiać integrację (plugin) z interfejsem VMware vSphere Web Client, umożliwiającą administratorom VMware zarządzanie backupem z poziomu tego interfejsu.
	6. W celu skrócenia czasu backupu środowiska VMware, oprogramowanie musi wykonywać wirtualne kopie syntetyczne korzystając z rejestru zmian (*Change Block Tracking*) oferowanego przez VADP. Oprogramowanie backupu musi każdorazowo ustalać listę segmentów danych, które zostały zmodyfikowane od ostatniej kopii zapasowej, a następnie odczytać i wysłać wyłącznie zmienione segmenty. Na podstawie zmienionych segmentów oraz wcześniejszej kopii zapasowej oprogramowanie backupu musi potrafić skonstruować nową pełną kopię zapasową. Kopia syntetyczna może być wykonywana w trybie inline lub w trybie post-process tj. uruchamiana po zakończeniu kopii przyrostowej lub według zadanego harmonogramu.
	7. Oprogramowanie backupu musi umożliwiać uruchomienie wirtualnej maszyny VMware wprost z kopii zapasowej bez konieczności kopiowania wszystkich danych odtwarzanej maszyny wirtualnej do środowiska produkcyjnego.
	8. Przy backupie środowisk VMware musi istnieć możliwość definiowania uniwersalnych warunków (kryteriów) celem automatycznego wyszukiwania maszyn wirtualnych.
	9. Oprogramowanie backupu musi oferować funkcjonalność odtwarzania pojedynczych plików z backupu całych maszyn wirtualnych z systemem operacyjnym Windows oraz Linux w środowisku VMware. Oznacza to backup całych dysków VMDK, a odtwarzanie z takiego backupu albo całej maszyny wirtualnej lub pojedynczych plików bez konieczności wykonywania jakichkolwiek dodatkowych backupów.
	10. Dla maszyn wirtualnych VMware z bazami danych MS SQL musi istnieć możliwość wykonywania backupu tzw. „application-aware” na poziomie obrazu maszyny wirtualnej z możliwością odtwarzania pojedynczych baz danych.
	11. Oprogramowanie backupu musi oferować integrację dla backupu środowisk wirtualnych opartych o Microsoft Hyper-V – backup na poziomie całych maszyn z możliwością przywracania pojedynczych plików z maszyn wirtualnych Windows z backupu całej maszyny wirtualnej (jednoprzebiegowy backup).
	12. Oprogramowanie backupu musi wspierać Microsoft Hyper-V 2012 R2, 2016, 2019, 2022.
	13. Proponowane rozwiązanie musi wspierać tworzenie syntetycznych kopii zapasowych (tworzonych na podstawie ostatniego pełnego i przyrostowego backupu RCT) maszyn wirtualnych Hyper-V w celu umożliwienia tworzenia kopii zapasowych przyrostowych na zawsze.
 |
| 17. | Oferowane urządzenie dyskowe | * 1. Dostarczane urządzenie dyskowe musi być typu PBBA (Purpose Built Backup Appliance) z zainstalowanym na nim oferowanym oprogramowaniem backupu lub urządzeniem deduplikującym zintegrowanym z oferowanym oprogramowaniem backupu przez specjalistyczne API. W obu przypadkach musi być dostępna co najmniej następująca funkcjonalność:
1. wykonywanie deduplikacji na klientach oprogramowania backupu (algorytmem urządzenia deduplikującego), lub równoważny zapewniający nieprzerwaną pracę serwerów produkcyjnych bez straty wydajności.
2. transfer danych bezpośrednio z klientów oprogramowania backupu do urządzenia deduplikującego zarówno przez sieć LAN jak i/lub FC SAN bez udziału jakichkolwiek serwerów pośredniczących,
3. wykonywanie wirtualnych kopii syntetycznych, zarządzanie replikacją danych pomiędzy urządzeniami deduplikującymi.
	1. W każdym przypadku oferowane urządzenie dyskowe oraz oprogramowanie backupu muszą pochodzić od jednego producenta i być wspierane przez jednego producenta.
	2. Urządzenie dyskowe musi posiadać mechanizm WORM w celu ochrony danych przed zaszyfrowaniem, modyfikacją i usunięciem przez złośliwe oprogramowanie. Funkcjonalność musi zapewniać, że obraz kopii zapasowej jest tylko do odczytu i nie może być modyfikowany, uszkodzony lub zaszyfrowany po utworzeniu kopii zapasowej oraz chronić obraz kopii zapasowej przed usunięciem przed upływem terminu ważności. Urządzenie musi posiadać certyfikat SEC17a-4(f).
	3. Funkcjonalność WORM musi być zarządzana przez oferowane oprogramowanie kopii zapasowych tj. zarządzanie czasem ochrony przechowywanych na urządzeniu obrazów kopii zapasowych odbywa się z poziomu oprogramowania backupu, a nie na poziomie urządzenia.
	4. Jeżeli oferowane urządzenie dyskowe wymaga dodatkowych licencji na wszystkie posiadane funkcjonalności lub pojemność muszą one zostać dostarczone.
	5. Pojemność użyteczna oferowanego urządzenia nie może być mniejsza niż 200TiB (base 2) tj. pojemność netto dostępna bezpośrednio w urządzeniu dla danych/kopii zapasowych – po odliczeniu przestrzeni wymaganych do działania urządzenia np. parzystości RAID/cache/dysków spare itd.
	6. Urządzenie musi umożliwiać wykonywanie backupu z wydajnością: min. 30TB/h w przypadku deduplikacji na urządzeniu,
	7. Urządzenie musi posiadać co najmniej następujące interfejsy sieciowe:

4 x 1GbE RJ45 4 x 25/10 10GbE optyczne,4 x FC16 lub 4x25/10 10GbE optyczne (w przypadku mechanizmów tworzenia kopii poprzez Ethernet) |
| 18 | Licencjonowanie | * 1. W ramach dostarczonych licencji musi być dostępna pełna funkcjonalność Systemu tj. spełnione wszystkie przedstawione wymagania.
	2. Należy dostarczyć licencje w ilości umożliwiającej backup 150 TB danych źródłowych ze środowisk wirtualnych VMware vSphere, Microsoft Hyper-V oraz 10 TB danych z serwerów fizycznych. Licencja ma w zależności od rozwiązania i przyjętej metody obliczeń dostarczona na 150 TB danych Front End z retencją min. 90 dni dla kopi dziennych.
	3. Licencje na rozwiązanie po okresie wsparcia nie wygasają oraz nieograniczane są żadne funkcjonalności związane z tworzeniem i odtwarzaniem kopii zapasowych
	4. W przypadku licencji subskrypcyjnych:
1. Dostarczone oprogramowanie backupu musi zapewnić pełną funkcjonalność, w tym możliwość wykonania nowych kopii zapasowych, zarządzania politykami kopi zapasowych oraz odtwarzania danych, niezależnie od statusu subskrypcji licencyjnej, do czasu uzyskania nowej licencji subskrypcyjnej.
2. Producent oprogramowania nie może stosować mechanizmów, które po wygaśnięciu subskrypcji ograniczają lub uniemożliwiają wykonywanie nowych operacji kopi zapasowych i przywracania danych. Obejmują one w szczególności

- brak blokady wykonywania nowych kopii zapasowych- brak ograniczeń w zakresie odtwarzania danych- możliwość zarządzania politykami retencji i harmonogramami kopii zapasowych- utrzymanie dostępu do wszystkich zapisanych danych- zachowanie pełnej funkcjonalności do czasu uzyskania nowej licencji subskrypcyjnej1. Zamawiający wymaga dokumentu od producenta Systemu, który potwierdzi, że po okresie 60 miesięcy warunki 18.4 a) i 18.4 b) będą spełnione. Dokument oświadczenia musi być dostarczony w oryginale i jeżeli jest w języku obcym przetłumaczony na język polski. Zamawiający zastrzega prawo potwierdzenia jego prawdziwości u Producenta przed wyborem oferty.
 |
| 19 | Gwarancja  | * 1. Oferowane sprzęt i oprogramowanie muszą być objęte wsparciem producenta przez okres 60 miesięcy od dnia podpisania końcowego protokołu odbioru.
	2. Wsparcie producenta dla sprzętu i oprogramowania musi umożliwiać zgłaszanie awarii i usterek w trybie 24 x 7, z czasem dostawy części w trybie następnego dnia roboczego od potwierdzenia awarii sprzętowej przez serwis producenta z usługą wymiany części na miejscu.
	3. Uszkodzone: dyski, pamięci flash, i inne nośniki danych z możliwością trwałego zapisu zostają u Zamawiającego.
	4. Ponadto w okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania, a także dostępu do dokumentacji producenta w trybie 24x7.
 |
| 20 | Reputacja | * 1. Rozwiązanie musi być w kwadracie Gartnera pod nazwą „Enterprise Backup and Recovery Software Solutions” w ćwiartce Leaders. w latach 2021, 2022, 2023, 2024
 |
| 21 | Wymagania dotyczące instalacji, konfiguracji i integracji urządzeń.Wdrożenie. | * 1. Wykonanie i przedstawienie do akceptacji Zamawiającego projektu wdrożenia Systemu.
	2. Montaż urządzeń w szafie RACK wskazanej przez Zamawiającego.
	3. Montaż urządzeń Systemu, podłączenie do zasilania i podpięcie do sieci komputerowej
	4. Wykonanie okablowania oraz podłączenie do istniejącej infrastruktury Zamawiającego.
 |
| 22 | Wymagania dodatkowe | * 1. Wszelkie wymagane komponenty (kable, listwy, wkładki, interfejsy, karty rozszerzeń, moduły, szyny, patchcordy itp.) niezbędne do uruchomienia Systemu i podłączenia do infrastruktury Zamawiającego muszą być dostarczone w ramach przedmiotu zamówienia i kompatybilne z infrastrukturą Zamawiającego
 |
| 23 | Szkolenie | * 1. Wykonawca dostarczy harmonogram i program szkolenia, (min. 7 dni przed szkoleniem) – do akceptacji Zamawiającego;
	2. Szkolenie Instruktażowe/stanowiskowe 2-dniowe po 8 godzin dla 3 administratorów wdrożonego Systemu w siedzibie Zamawiającego lub w trybie zdalnym w języku polskim
	3. Szkolenie certyfikowane produktowe z wdrożonej technologii dla administratorów wdrożonego Systemu:
1. poziom podstawowy minimum 3 dni po 8 godzin z wdrożonego rozwiązania – minimum 3 osoby,
2. poziom zaawansowany minimum 3 dni po 8 godzin z wdrożonego rozwiązania – minimum 3 osoby.
	1. W przypadku, gdy Wykonawca zaproponuje przeprowadzenie szkolenia poza miejscem realizacji umowy tj. poza siedzibą (miejscowością) Zamawiającego jest zobowiązany do zapewnienia dojazdu do tego miejsca, zakwaterowanie uczestników, ich wyżywienie oraz powrót.
	2. Szkolenia z Systemu muszą być przeprowadzone w języku polskim na terenie RP.
	3. Szkolenia z Systemu muszą zostać przeprowadzone i zakończone przed podpisaniem końcowego protokołu odbioru umowy
	4. Wykonawca dostarczy materiały szkoleniowe.
	5. Minimum 2 letnie doświadczenie szkolącego w administrowaniu z wdrażanego Systemu.
	6. Wiedza szkolącego potwierdzona certyfikatem Producenta rozwiązania na poziomie min. zaawansowanym.
 |
| 24 | Dokumentacja | * 1. Dokumentacja powykonawcza musi odzwierciedlać stan faktyczny Systemu w momencie zakończenia prac wdrożeniowych. Musi zawierać m.in.:

Opis architektury połączeń fizycznych:1. Opis skonfigurowanych wymaganych funkcjonalności podczas wdrożenia.
2. Opis koncepcji i architektury rozwiązania,
3. Specyfikacja środowiskowa dostarczonego sprzętu,
4. Opis konfiguracji sprzętowej i podłączenia do sieci LAN i SAN Zamawiającego,
5. Opis konfiguracji logicznej urządzeń i oprogramowania backupu,
6. Zestawienie adresacji sieciowej,
7. Opis konfiguracji polityk backupu.
	1. Dokumentacja musi być wykonana w formie minimum elektronicznej.
	2. Zamawiający wymaga przygotowania przez Wykonawcę min. 10 procedur eksploatacyjnych i awaryjnych w tym procedury odtwarzania danych.
	3. Zamawiający wymaga udokumentowania parametrów technicznych i wymaganych funkcjonalności Systemu poprzez karty katalogowe producenta urządzeń lub oświadczenie producenta urządzenia/oprogramowania.
 |
| 25 | Wdrożenie | * 1. Dostarczenie projektu technicznego przedwdrożeniowego zawierającego co najmniej:
1. Opis koncepcji i architektury rozwiązania,
2. Specyfikacja środowiskowa dostarczonego sprzętu – na potrzeby przygotowania serwerowni przez Zamawiającego,
3. Opis konfiguracji sprzętowej i podłączenia do sieci LAN i SAN Zamawiającego,
4. Opis konfiguracji logicznej urządzeń oraz oprogramowania backupu,
5. Zestawienie adresacji sieciowej,
6. Opis konfiguracji polityk backupu,
7. Zestawienie procedur eksploatacyjnych i awaryjnych,
8. Zestawienie scenariuszy testowych.
9. Instalacja i konfiguracja oprogramowania backupu.
	1. Integracja Systemu z infrastrukturą Zamawiającego.
	2. Objęcie kopią zapasową systemów Zamawiającego w tym instalacja agentów backupu, konfiguracja polityk itd.
	3. Testy funkcjonalne rozwiązania w tym odtwarzania danych.
 |

**Wymagania minimalne dla biblioteki taśmowej LTO**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa wymogu** | **Wymagane minimalne parametry techniczne sprzętu** |
| 1. | Ogólne | Urządzenie taśmowe umożliwiające przechowywanie danych na nośnikach taśmowych typu LTO. |
| 2. | Obudowa | 1. Po rozbudowie pomiędzy poszczególnymi modułami biblioteki musi być możliwość automatycznego przemieszczania nośników z wykorzystaniem jednego robota, który musi mieć dostęp do wszystkich kieszeni na nośniki.
2. Biblioteka musi być wyposażona w zestaw umożliwiający jej zamontowanie w szafie Rack 19” oraz komplet niezbędnego okablowania, wkładek itp. do podłączenia w infrastrukturze zamawiającego
 |
| 3. | Napędy i obsługiwane nośniki | 1. Biblioteka musi być wyposażona w minimum trzy napędy taśmowe w technologii LTO8.
2. Musi umożliwiać wymianę napędów bez przerwania pracy biblioteki.
3. Minimalna pojemność taśmy bez kompresji 12TB bez kompresji.
4. Każdy z napędów taśmowych musi posiadać interfejs FC o prędkości minimum 8Gb/s.
 |
| 4. | Kieszenie na nośniki (sloty) | 1. Biblioteka musi mieć minimum 50 kieszeni na nośniki, jeśli ich obsługa wymaga dodatkowych licencji wymagane jest dostarczenie takiej licencji.
2. Biblioteka musi mieć możliwość zdefiniowania co najmniej 1 kieszeni typu „mail slot”.
 |
| 5. | Rozbudowa | 1. Ze względu na przyszłościowe zastosowanie wymaga się, aby biblioteka miała możliwość rozbudowy do minimum 20 napędów taśmowych i była w stanie obsłużyć co najmniej 250 slotów wspólnie zarządzanych przez jeden moduł kontrolny.
 |
| 6. | Zarządzanie | 1. Biblioteka musi być wyposażona w moduł zdalnego zarządzania.
2. Biblioteka musi udostępniać funkcję monitorowania napędów.
3. Biblioteka musi mieć możliwość zdalnego monitorowania urządzenia i wychwytywania błędów bezpośrednio przez inżynierów producenta/autoryzowany serwis za pomocą odpowiedniego oprogramowania.
 |
| 7. | Pozostałe wymagania | 1. Biblioteka musi posiadać czytnik kodów kreskowych do identyfikacji taśm.
2. Biblioteka musi zostać dostarczona z redundantnym zasilaniem.
3. Biblioteka musi szyfrować dane kluczem o sile AES-256.
4. Biblioteka powinna być wykonana w technologii umożliwiającej sprzętowy podział na mniejsze biblioteki „logiczne”, a następnie podłączanie do różnych serwerów, korzystając różnego oprogramowania do wykonywania kopii zapasowych i archiwizacji.
5. Biblioteka musi mieć interfejsy min. FC 8 GB/s do transferu danych i LAN 1 GB/s – do zarządzania
 |
| 8. | Gwarancja | 1. Biblioteka musi być objęta minimum 5 letnią gwarancją i wsparciem producenta biblioteki lub autoryzowanego serwisu producenta z możliwością zgłaszania awarii w trybie 24 x 7 w języku polskim, z czasem dostawy części w trybie następnego dnia roboczego z usługą wymiany części na miejscu.)
2. W okresie serwisu zamawiający musi mieć dostęp do zdalnej pomocy technicznej, poprawek i nowych wersji oprogramowania i sterowników oferowanej biblioteki.
 |