Załącznik nr 1 do SWZ

Przedmiotem zamówienia jest dostawa serwera kopii bezpieczeństwa wraz z oprogramowaniem systemowym, o podanych poniżej parametrach.

Całość rozwiązania ma być w pełni kompatybilna z posiadanym przez Zamawiającego systemem kopii bezpieczeństwa opartym o oprogramowanie Dell EMC Data Protection Suite for VMware oraz urządzenia Dell EMC DataDomain 6300 (2szt.).

1. Serwer kopii bezpieczeństwa – 1 szt.

Lp.	Opis
1.	Urządzenie musi zostać dostarczone w stanie kompletnym (zgodnie ze specyfikacją), z zainstalowanym najnowszym oprogramowaniem, kompatybilnym z aplikacjami wykorzystywanymi przez Zamawiającego, oraz z licencjami umożliwiającymi uruchomienie wyspecyfikowanych funkcjonalności urządzenia.
2.	Urządzenie musi zapewniać możliwość montażu w szafie rack 19". Zamawiający wymaga dostarczenia wszystkich elementów koniecznych do instalacji takich jak: prowadnice/szyny, śruby montażowe, kable podłączeniowe z wyjątkiem kabli LAN które zostaną zapewnione przez Zamawiającego.
3.	Urządzenie musi oferować przestrzeń min. 60 TB netto (powierzchni użytkowej do wykorzystania przez Zamawiającego na deduplikanty, fizyczna), wymagana skalowalność do min. 170 TB pojemności netto na deduplikanty, fizyczna.
4.	Wraz z uruchomioną (zalicencjonowaną) pojemnością użytkową do wykorzystania przez Zamawiającego muszą być dostarczone, w nie mniejszej ilości niż uruchomiona pojemność, licencje na następujące funkcjonalności: kompresja, wykonywanie snapshotów, deduplikacja na źródle, szyfrowanie, replikacja i blokowanie retencji (retention lock).
5.	Urządzenie musi posiadać minimum: • 4 porty Ethernet 10 Gb/s SFP+, wymagana możliwość obsługi każdym portem Ethernet protokołów CIFS, NFS, z deduplikacją na źródle; • 4 porty Ethernet 10 Gb/s RJ-45, wymagana możliwość obsługi każdym portem Ethernet protokołów CIFS, NFS, z deduplikacją na źródle;
6.	Urządzenie musi umożliwiać jednoczesny dostęp i obsługę protokołów: CIFS, NFS, deduplikacja na źródle. Jeżeli wymaga to licencji, to muszą być one dostarczone wraz z licencjami dla dostarczonej/uruchomionej zalicencjonowanej) pojemności netto.
7.	Urządzenie musi osiągać zagregowaną wydajność (dla pełnej konfiguracji) protokołami: NFS co najmniej 10 TB/h (dane podawane przez producenta) oraz co najmniej 25 TB/h z wykorzystaniem deduplikacji na źródle (podawane przez producenta w oficjalnych i dostępnych publicznie materiałach).

8.	Urządzenie musi pozwalać na jednoczesną obsługę minimum 250 strumieni w tym jednocześnie: zapis danych minimum 150 strumieniami / odczyt danych minimum 50 strumieniami / replikacja minimum 50 strumieniami pochodzących z różnych aplikacji oraz dowolnych protokołów (CIFS, NFS, deduplikacja na źródle) oraz dowolnych interfejsów w tym samym czasie. Wymienione wartości 250 jednoczesnych strumieni dla wszystkich protokołów (czyli jednocześnie 150 dla zapisu i jednocześnie 50 strumieni dla odczytu i jednocześnie 50 strumieni dla replikacji) musi mieścić w przedziale oficjalnie rekomendowanym i wspieranym przez producenta urządzenia. Wszystkie zapisywane strumienie muszą podlegać globalnej deduplikacji przed zapisem na dysk (in-line) jak opisano w niniejszej specyfikacji.
9.	Urządzenie musi deduplikować dane in-line przed zapisem na nośnik dyskowy, przy czym na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia.
10.	Urządzenie musi posiadać obsługę mechanizmów globalnej deduplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, deduplikacja na źródle) przechowywanych w obrębie całego urządzenia co oznacza, że przechowywany na urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany.
11.	Urządzenie musi posiadać obsługę mechanizmów globalnej deduplikacji pomiędzy dowolnymi dwoma (i więcej) wirtualnymi bibliotekami emulowanymi w obrębie tego samego urządzenia. Blok danych otrzymany i zapisany w wirtualnej bibliotece A, nie może zostać ponownie zapisany jeśli trafi do innej wirtualnej biblioteki (wirtualnej biblioteki B) w obrębie tego samego urządzenia (to samo dotyczy udziałów NFS/CIFS).
12.	Przestrzeń składowania zdeduplikowanych danych musi być jedna dla wszystkich protokołów dostępowych, co oznacza zastosowanie pojedynczej bazy deduplikatów bez względu na ilość/rodzaj używanych protokołów dostępowych.
13.	Proces deduplikacji musi odbywać się w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie zapisane jeszcze na system dyskowy urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych.
14.	Proponowane rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej) w celu ich późniejszej deduplikacji (wymagana deduplikacja in-line).
15.	Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo kompresowane.
16.	Urządzenie musi wspierać (wymagane jest formalne wsparcie producenta urządzenia), co najmniej następujące aplikacje: Dell EMC Networker, Dell EMC Avamar, Oracle RMAN, Microsoft SQL Server Management Studio.
17.	W przypadku deduplikacji na źródle poprzez sieci LAN oraz WAN, wymagana jest możliwość szyfrowania komunikacji kluczem minimum 256 bitów.

18.	Urządzenie powinno umożliwiać zaszyfrowanie przechowywanych danych, wymagane są dodatkowe licencje umożliwiające zaszyfrowanie i przechowywanie zaszyfrowanych danych dla dostarczonej/uruchomionej zalicencjonowanej pojemności netto.
19.	Urządzenie nie może zmniejszać swojej wydajności w czasie przybywania kolejnych danych o więcej niż 5%.
20.	Urządzenie musi umożliwiać bezpośrednią replikację danych do drugiego urządzenia takiego samego typu. Konfiguracja replikacji musi być możliwa w każdym z trybów: „1:1”, „1:n”, „n:1”, kaskadowo (urządzenie A replikuje dane do urządzenia B, które te same dane replikuje do urządzenia C)
21.	Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu. Jeżeli wymaga to licencji, to muszą być one dostarczone dla dostarczonej/uruchomionej zalicencjonowanej pojemności netto.
22.	Urządzenie musi umożliwiać bezpośrednią dwukierunkową replikację składowanych danych z posiadanymi przez Zamawiającego dwoma urządzeniami Dell EMC DataDomain 6300. Replikacji powinny podlegać jedynie bloki (deduplikanty), które nie znajdują się na urządzeniu docelowym mechanizmu replikacji. Jako rozwiązanie równoważne – w przypadku braku możliwości realizacji powyżej opisanej dwukierunkowej replikacji deduplikantów z posiadanymi przez Zamawiającego urządzeniami Dell EMC DataDomain 6300 – dopuszcza się dostarczenie dwóch jednakowych pełnych kompletów serwerów kopii bezpieczeństwa spełniających wszystkie pozostałe wymagania niniejszego postępowania i posiadające możliwość takiej replikacji.
23.	Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych do replikacji.
24.	W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie danych kopii bezpieczeństwa, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami.
25.	Oferowane urządzenie musi działać poprawnie (muszą być dostępne wszystkie jego funkcje i utrzymane parametry użytkowe) przy zapełnieniu danymi na poziomie co najmniej 90%. Dokumentacja urządzenia nie może wskazywać na ew. problemy, obostrzenia, które są efektem zapełnienia urządzenia zabezpieczanymi danymi, na poziomie mniejszym niż 90%
26.	Narzut na wydajność związany z replikacją nie może zmniejszyć wydajności urządzenia o więcej niż 10%.
27.	Wymagana jest możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami.
28.	Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 bądź równoważnej.

29.	Wymagana jest możliwość zaprezentowania każdej z logicznych części urządzenia jako niezależnego urządzenia dostępnego za pośrednictwem: CIFS, NFS, deduplikacji na źródle.
30.	Urządzenie musi umożliwiać zdefiniowanie blokady skasowania danych (funkcjonalność WORM). Blokada skasowania danych musi chronić plik w zdefiniowanym czasie przed usunięciem/modyfikacją pliku. Blokada skasowania danych musi działać w dwóch trybach (do wyboru przez administratora, jeżeli wymaga to licencji, to muszą być one dostarczone dla zalicencjonowanej dostarczonej pojemności netto): • Możliwość zdjęcia blokady przed upływem ważności danych • Brak możliwości zdjęcia blokady przed upływem ważności danych
31.	Urządzenie musi weryfikować dane po zapisie (nie chodzi o ew. weryfikację danych indeksowych generowanych przez urządzenie, ale o weryfikację wszystkich zabezpieczanych danych backup'owych). Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie. Powyższa weryfikacja powinna być realizowana w locie, czyli przed usunięciem z pamięci oryginalnych danych (otrzymanych z aplikacji backupowej), musi być realizowana w trybie ciągłym (a nie ad-hoc), wymagane parametry wydajnościowe urządzenia muszą uwzględniać tę funkcjonalność. Wymaga się potwierdzenie opisanej funkcjonalności w oficjalnej dokumentacji producenta oferowanego urządzenia – należy podać link do ww. dokumentacji w Formularzu Ofertowym – Załącznik nr 1 do SWZ.
32.	Urządzenie musi automatycznie (samoczynnie) wykonywać sprawdzanie spójności danych po zapisaniu danych na dysk oraz rozpoznawać i naprawiać błędy „w locie". Każde zapisane na fizycznych dyskach dane muszą być odczytane i porównane z danymi otrzymanymi. Proces ten musi odbywać się „w locie" – musi być elementem procesu zapisu danych przez urządzenie.
33.	Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia.
34.	Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać procesów: backupu i odtwarzania danych (zapisu oraz odczytu danych z zewnątrz do systemu).
35.	Urządzenie musi mieć możliwość zdefiniowania dla procesu usuwania przeterminowanych danych (czyszczenia): maksymalnego obciążenia (poziomu obciążenia procesora) harmonogramu, w którym się będzie odbywać
36.	Standardowa częstotliwość usuwania przeterminowanych danych (czyszczenie) nie powinna być większa niż 1 raz na tydzień - minimalizując w ten sposób czas w którym backupy/odtwarzania narażone są na spowolnienie.
37.	Po niespodziewanym wyłączeniu prądu i ponownym uruchomieniu, urządzenie musi być gotowe do przyjmowania danych (kopie bezpieczeństwa, archiwa) w czasie nie dłuższym niż 60 minut od włączenia.
38.	Urządzenie musi mieć możliwość zarządzania poprzez: • interfejs graficzny dostępny z przeglądarki internetowej • linię komend (CLI) dostępną z poziomu ssh (secure shell)

39.	Oprogramowanie do zarządzania musi rezydować na oferowanym urządzeniu.
40.	Zasilanie urządzenia musi być redundantne (lub nadmiarowe), a jego naprawa/wymiana nie może powodować wyłączenia/zablokowania zapisu/odczytu z urządzenia.
41.	Urządzenie musi umożliwiać wykonywanie SnapShot'ów, czyli umożliwiać zamrożenie obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane urządzenie musi również umożliwiać odtworzenie danych ze Snapshot'u. Odtworzenie danych ze Snapshot'u nie może wymagać konieczności nadpisania danych produkcyjnych jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania/odtwarzania backupów). Urządzenie musi pozwalać na przechowywanie minimum 700 Snapshotów jednocześnie w obrębie oferowanej przestrzeni, przy zachowaniu globalnej deduplikacji oraz standardowego trybu pracy urządzenia – umożliwiającego wykorzystanie wszystkich dostępnych funkcjonalności.
42.	Urządzenie musi umożliwiać podział na logiczne części. Dane znajdujące się w każdej logicznej części muszą być między sobą deduplikowane (globalna deduplikacja między logicznymi częściami urządzenia). Minimalna ilość logicznych części pracujących równolegle musi wynosić nie mniej niż 10. Producent musi oficjalnie wspierać tę ilość logicznych części pracujących równolegle z pełną wydajnością urządzenia.
43.	Oprogramowanie do deduplikacji na źródle musi spełniać następujące wymagania: • w przypadku współpracy z RMAN (dla Oracle) lub Microsoft SQL Management Studio, urządzenie musi umożliwiać deduplikację na źródle i przesłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN, • deduplikacja danych odbywa się na dowolnym serwerze posiadającym funkcjonalność Media Agenta/ klienta / serwera RMAN / serwera SQL. • deduplikacja w wyżej wymienionych przypadkach musi zapewniać aby z serwerów do urządzenia były transmitowane poprzez sieć tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu.

44.	Urządzenie musi umożliwiać utworzenie warstwy przestrzeni do składowania danych kopii bezpieczeństwa z wykorzystaniem nośników taśmowych przy wykorzystaniu minimum dwóch napędów wykonanych w technologii LTO-9, oraz umożliwiać zapis i/lub odczyt dowolnego z minimum 45 nośników dostępnych w urządzeniu. Musi istnieć możliwość rozbudowy o dodatkowe miejsca na nośniki taśmowe. Zamawiający uzna za równoważny typ napędu, który spełni następujące kryteria: • umożliwia zapisanie w natywny sposób (bez kompresji itp.) minimum 15TB danych, • maksymalna prędkość zapisu danych bez kompresji wynosząca min. 370 MB/s, • musi umożliwiać zapis na nośniki jednokrotnego zapisu (ang. WORM), • musi umożliwiać wykorzystanie kompresji sprzętowej na poziomie min. 2,5:1. Moduł musi umożliwiać wymianę napędów bez przerywania pracy (napędy typu „hot swap"). Urządzenie musi pozwalać na wyjęcie lub włożenie do urządzenia minimum 5 nośników jednocześnie bez zajmowania miejsc dla minimalnej wymaganej liczby nośników, przy czym musi być możliwość zwiększenia tej liczby. Dopuszcza się zastosowanie modułów umożliwiających utworzenie warstwy przestrzeni do składowania danych kopii bezpieczeństwa z wykorzystaniem nośników taśmowych dedykowanych do tego celu, jeżeli obudowa oferowanego urządzenia nie umożliwia instalacji napędów taśmowych w wymaganej ilości. Minimalne wymagania dla modułów umożliwiających utworzenie warstwy przestrzeni do składowania danych kopii bezpieczeństwa z wykorzystaniem nośników taśmowych: Pojedynczy moduł w dostarczonej konfiguracji nie może przekraczać wysokości 3U. Montaż w przemysłowej szafie RACK 19". Moduł musi umożliwiać rozbudowę do min. 8 modułów, 3U każdy, minimum 24U łącznie. Niedopuszczalne jest stosowanie jakiegokolwiek okablowania zewnętrznego (np. łączników SCSI) do wykonania rozbudowy, wszelka komunikacja musi odbywać się połączeniami wewnętrznymi. Moduł musi być wyposażony w min. 2 napędy taśmowe LTO-9 połowy wysokości (Half Height) lub wykonane w technologii gwarantującej co najmniej taką samą pojemność, poziom kompresji oraz prędkość zapisu i odczytu danych, wyposażone w natywny interfejs FC 8Gbps. Żadna funkcjonalność modułu realizowana przez napędy taśmowe (np. sprawdzanie konsystencji danych) nie może wymuszać łączności napędów taśmowych do innych przełączników niż przełączniki FC. Moduł musi mieć możliwość rozbudowy do minimum 24 napędów taśmowych LTO8 (o natywnym interfejsie SAS lub/i FC, połowy wysokości (Half Height)), łącznie. Musi być możliwość mieszania napędów różnych technologii LTO (od min. LTO-7) oraz różnych interfejsów.

	Moduł musi być wyposażony w minimum 50 kieszeni na nośniki taśmowe z czego 50 kieszeni musi być zalicencjonowanych do dowolnego użytku. Moduł musi mieć możliwość rozbudowy do minimum (fizycznie oraz zalicencjonowanych do dowolnego użytku) 400 kieszeni na nośniki taśmowe. Moduł musi mieć możliwość zdefiniowania do 25 kieszeni typu „mail slot/import/export" w odstępach co 5 (licząc od 0). Moduł musi być zarządzany z poziomu panelu dotykowego zabezpieczonego hasłem lub/i numerem PIN oraz zdalnego interfejsu zarządzania przez panel WWW (HTML5). Moduł musi wspierać Multi-Factor Authentication (MFA) dla min. użytkowników lokalnych. Musi być możliwość tworzenia użytkowników lokalnych oraz integracji z systemem usług katalogowych – Microsoft Active Directory. Moduł musi udostępniać funkcje monitorowania stanu napędów i robota. Moduł musi mieć możliwość zdalnego monitorowania stanu urządzenia i wychwytywania błędów bezpośrednio przez inżynierów producenta za pomocą odpowiedniego oprogramowania, dostarczonego razem z modułem archiwizującym. Nie jest dopuszczalne instalowanie żadnych dodatkowych systemów (wirtualnych czy fizycznych) w celu osiągnięcia tej funkcjonalności. Obsługa protokołów min. SNMP, Syslog. Moduł archiwizujący musi posiadać min. 1 interfejs 1GbE do zarządzania. Interfejs musi być zlokalizowany na karcie zarządzania modułem archiwizującym oraz posiadać wszystkie mechanizmy zarządzania na obu portach. Moduł musi być wykonany w technologii umożliwiającej sprzętowy podział na części „logiczne", a następnie podłączane do różnych serwerów, korzystających z różnego oprogramowania do wykonywania kopii zapasowych i archiwizacji. Moduł musi wspierać do 21 „logicznych instancji". Moduł musi być wyposażony w czytnik kodów kreskowych W pełni redundantne dla wszystkich modułów w których zamontowane będą napędy taśmowe. Moduł powinien być dostarczony wraz z 50 taśmami LTO-9 oraz 1 taśmą czyszczącą. Moduł musi mieć możliwość włączenia adresacji logicznej dla jego modułu kontrolnego (numer seryjny) oraz napędów taśmowych (WWN), dzięki czemu wymiana tych komponentów nie wpływa na rekonfigurację aplikacji i sieci SAN. Moduł musi mieć możliwość definiowania tzw. "logical lock", który uniemożliwi użytkownikowi administracyjnemu przesunięcie nośnika taśmowego w inny slot lub napęd modułu zapisu na taśmę. Moduł musi mieć możliwość zainstalowania tzw. "hardware lock", który uniemożliwi fizyczną ingerencję w tenże moduł (np. serwisowe wysunięcie magazynków z nośnikami taśmowymi).

45.	Dostarczony serwer kopii bezpieczeństwa musi być serwisowany przez autoryzowany serwis producenta ze wsparciem przez okres 5 lat, w dni robocze, z reakcją najpóźniej następnego dnia roboczego. W ramach wsparcia Zamawiający otrzyma również możliwość bezpłatnego otrzymywania aktualizacji oprogramowania urządzeń w okresie obowiązywania wsparcia. W wypadku wymiany uszkodzonych dysków twardych przez serwis producenta, uszkodzone dyski pozostają u Zamawiającego. W przypadku zastosowania dedykowanego modułu umożliwiającego utworzenie warstwy przestrzeni do składowania danych kopii bezpieczeństwa z wykorzystaniem nośników taśmowych, moduł ten musi być objęty wsparciem i gwarancją jego producenta z czasem reakcji następnego dnia roboczego (NBD) przez okres co najmniej 5 lat.

2. Serwer kopii bezpieczeństwa – oprogramowanie systemowe – 1 komplet

Lp.	Opis
1.	Wymagane jest dostarczenie oprogramowania systemowego serwera kopii bezpieczeństwa: • umożliwiającego instalację dwóch instancji modułów zarządzających procesem tworzenia kopii bezpieczeństwa w dwóch lokalizacjach, wraz z replikacją danych kopii bezpieczeństwa pomiędzy tymi instancjami, • umożliwiającego instalację instancji modułu zarządzającego procesem tworzenia kopii bezpieczeństwa obsługującego zapis na nośniki taśmowe, • umożliwiającego stworzenie systemu raportującego, • umożliwiającego zaindeksowanie oraz przeszukiwanie danych backupowych, • umożliwiającego stworzenie rozwiązania Continuous Data Protection (CDP) dla środowisk VMware, • umożliwiającego zarządzanie oferowanym środowiskiem dedykowanym do zabezpieczania danych.
2.	Wymagane jest dostarczenie wsparcia na oferowane oprogramowanie systemowe, realizowane przez producenta w okresie min. 5 lat w trybie 9x5 NBD, gwarantujące dostęp do najnowszych wersji oprogramowania.
3.	Wymagane jest dostarczenie licencji w/w oprogramowania dla środowiska obejmującego zarówno maszyny-komputery niezwirtualizowane oraz zwirtualizowane, charakteryzujące się sumaryczną ilością: 18 fizycznych procesorów (ang. CPU). Licencje będące przedmiotem postępowania muszą umożliwić zabezpieczenie (realizacje kopii bezpieczeństwa i ich odtwarzania) dowolnej ilości maszyn wirtualnych pracujących w środowisku liczącym minimum 18 fizycznych procesorów (ang. CPU). **Nie dopuszcza się licencji w modelu subskrypcyjnym.**
4.	Oprogramowanie musi wspierać (wymagane wsparcie producenta) następujące systemy operacyjne: Windows (także Microsoft Cluster), Linux (Red Hat, SUSE, Debian, CentOS, Ubuntu). Backup zasobów plików w przypadku powyższych systemów musi podlegać deduplikacji ze zmiennym blokiem na zabezpieczanej maszynie.

5.	Oprogramowanie musi wspierać (wymagane wsparcie producenta) backup online następujących baz danych i aplikacji: MS Exchange, MS SQL, Oracle, SharePoint, VMware vSphere, Hyper-V. Realizacja kopii bezpieczeństwa powyższych baz danych i aplikacji musi podlegać deduplikacji ze zmiennym blokiem na zabezpieczanej maszynie.
6.	Kopie bezpieczeństwa zabezpieczanych serwerów muszą być zapisywane bezpośrednio na dyski serwera kopii bezpieczeństwa będącego przedmiotem niniejszego zamówienia, bez pośrednictwa jakichkolwiek innych urządzeń/serwerów, dostarczone licencje muszą umożliwiać całkowitą utylizację wymaganej przestrzeni serwera.
7.	Oprogramowanie musi umożliwiać dla sieci lokalnej wykonanie kopii bezpieczeństwa: • pojedynczych plików, • całych systemów plików, • baz danych w trakcie ich normalnej pracy, • ustawień systemu operacyjnego Windows, • całych obrazów maszyn wirtualnych systemu VMware vSphere, • całych obrazów maszyn wirtualnych systemu Hyper-V.
8.	Oprogramowanie musi umożliwiać odtworzenie: • plików, • baz danych, na docelową maszynę - z poziomu centralnej konsoli systemu backupowego; wymagany scenariusz nie może wymagać logowania się na odtwarzaną maszynę w celu odtworzenia danych z serwera kopii bezpieczeństwa, • pojedynczych maili z kopii systemu poczty MS Exchange na docelową maszynę.
9.	Wymaga się aby oprogramowanie przesyłało na oferowany serwer kopii bezpieczeństwa tylko unikalne bloki nie znajdujące się na tym urządzeniu, w efekcie skracając czas backupu, obciążenie procesora i zmniejszając ruch w sieci WAN / LAN.
10.	Oprogramowanie nie może odczytywać tych plików z systemu dyskowego, które się nie zmieniły w stosunku do ostatniego backupu. Raz zabezpieczony plik nie może być ponownie odczytywany, chyba, że zmieni się jego zawartość.
11.	Wymagana jest możliwość definiowania w konsoli oprogramowania ważności (retencji) danych (backupów) na podstawie kryteriów czasowych (dni, miesiące, lata). Po okresie ważności kopie bezpieczeństwa muszą być automatycznie usunięte.
12.	Wymagana jest możliwość tworzenia z poziomu GUI (konsoli graficznej), polityk typu „dziadek – ojciec – syn”, to znaczy tworzenia polityk w których zdefiniowano: • Czas przechowywania dziennych kopii bezpieczeństwa • Czas przechowywania tygodniowych kopii bezpieczeństwa • Czas przechowywania miesięcznych kopii bezpieczeństwa • Czas przechowywania rocznych kopii bezpieczeństwa
13.	Konsola zarządzająca procesem tworzenia kopii bezpieczeństwa musi integrować się z Active Directory. Musi być możliwość przydzielania użytkownikom i grupom Active Directory dostępnych ról (min: administrator, monitoring, tylko odtwarzanie danych).
14.	Wymagana jest możliwość generowania (poprzez konsolę) raportów określających zajętość przestrzeni oferowanego serwera kopii bezpieczeństwa.
15.	Bloki przesyłane z zabezpieczanych serwerów do oferowanego serwera kopii bezpieczeństwa muszą być kompresowane i szyfrowane algorytmem z kluczem minimum 256-bitowym.
16.	Wymagana jest możliwość autentykacji komunikacji między klientem, a serwerem kopii bezpieczeństwa oparta na certyfikatach.
17.	Oprogramowanie musi wspierać realizację kopii bezpieczeństwa wirtualnych maszyn i ich odtwarzanie dla środowisk VMware vSphere min. 6.7, 7.

	Oprogramowanie musi umożliwiać w przypadku środowisk VMware następujące typy realizacji kopii bezpieczeństwa: • kopia bezpieczeństwa całych maszyn wirtualnych, • kopia bezpieczeństwa pojedynczych, wybranych dysków maszyny wirtualnej vmdk, • musi istnieć możliwość zastosowania wyrażeń regularnych do określenia które wirtualne dyski VMware mają podlegać kopii bezpieczeństwa, • w trakcie procesu realizacji kopii bezpieczeństwa odczytowi z systemu dyskowego mają podlegać tylko zmienione bloki wirtualnych maszyn systemu VMware (wymagane wykorzystanie mechanizmu CBT systemu VMware), • wykonywanie kopii bezpieczeństwa obrazów maszyn wirtualnych VMware nie może wymagać bufora dyskowego na kopię obrazów maszyn wirtualnych (plików vmdk). Powyższe metody realizacji kopii bezpieczeństwa maszyn wirtualnych muszą podlegać deduplikacji ze zmiennym blokiem przed wysłaniem danych do oferowanego serwera kopii bezpieczeństwa zgodnie z przytoczonymi wymaganiami. Powyższe metody realizacji kopii bezpieczeństwa muszą być wbudowane w oferowane oprogramowanie i nie powinny wymagać tworzenia skryptów/dodatkowych komend lub stosowania oprogramowania firm trzecich.
18.	Oferowane oprogramowanie musi pozwalać na szybkie odtworzenie: • całych obrazów maszyn wirtualnych, • pojedynczych dysków maszyny wirtualnej z kopii bezpieczeństwa całej maszyny wirtualnej.
19.	Wymaga się aby oferowane oprogramowanie umożliwiało odtwarzanie obrazów maszyn wirtualnych VMware z następującymi funkcjonalnościami: • odtwarzanie całych maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMware – odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od wykonania ostatniej kopii bezpieczeństwa, • odtwarzanie pojedynczych dysków maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMware – odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniej kopii bezpieczeństwa, • odtworzenie pojedynczych plików z kopii bezpieczeństwa obrazu maszyny wirtualnej bez konieczności odtworzenia całej maszyny wirtualnej, funkcjonalność ta musi być dostępna dla obrazów maszyn wirtualnych z zainstalowanym systemem operacyjnym Windows oraz Linux, Powyższe metody realizacji kopii bezpieczeństwa muszą być wbudowane w oferowane oprogramowanie i nie powinny wymagać tworzenia skryptów/dodatkowych komend.
20.	Oferowane oprogramowanie musi mieć możliwość prezentacji (bez konieczności odtworzenia) składowanych kopii bezpieczeństwa obrazów maszyn wirtualnych VMware (plików vmdk) jako katalogów na maszynie fizycznej w celu ich przeszukiwania (wymagane przeszukiwanie po nazwach plików jak również zawartości plików) z poziomu systemu operacyjnego maszyny fizycznej.
21.	Oferowane oprogramowanie musi mieć możliwość tworzenia kopii bezpieczeństwa/odtworzenia w trybie „image backup” (backup plików vmdk) maszyn wirtualnych znajdujących się na serwerach VMware ESX bez udziału vCenter.
22.	Oprogramowanie musi umożliwiać zdefiniowanie polityk wykonywania kopii, dostępnych dla administratora systemu VMware z poziomu vCenter. Administrator VMware musi mieć możliwość przyporządkowania nowo tworzonych maszyn wirtualnych do polityk wykonywania kopii.

23.	Oferowane oprogramowanie musi automatycznie naprawiać problemy związane ze snapshotami VMware. W przypadku gdy system VMware nie usunie snapshotu, oferowane oprogramowanie musi automatycznie ponawiać usunięcie snapshotu, a w przypadku konieczności automatycznie konsolidować maszyny wirtualne VMware vSphere.
24.	W przypadku systemów Windows Server wymagana funkcjonalność Bare Metal Recovery - automatycznego odtworzenia całego serwera (system operacyjny + ustawienia systemu operacyjnego + dane) w jednym kroku bezpośrednio z serwera kopii bezpieczeństwa.
25.	Oferowane oprogramowanie musi być dostępne (dla realizacji kopii bezpieczeństwa i odtwarzania) przez 24h na dobę, 7 dni w tygodniu. Wyklucza się istnienie okresów w przypadku których system realizacji kopii bezpieczeństwa nie może wykonywać kopii lub odtwarzania (tzw. BLACKOUT WINDOW).
26.	Wymaga się aby oferowane oprogramowanie posiadało możliwość bezpośredniego raportowania o błędach do serwisu producenta
27.	W ramach dostarczonych licencji musi być zapewniona możliwość monitorowania, raportowania, szczegółowego rozliczania z użycia komponentów systemu realizującego kopie bezpieczeństwa oraz analizy błędów dla środowiska kopii zapasowej Zamawiającego. Wymagana dostępność następujących raportów: • podsumowanie zadań kopii bezpieczeństwa (liczba backupów udanych, nieudanych, aktywnych, łączny rozmiar danych wykonanych kopii), • podsumowanie zadań odtworzeniowych (liczba odtworzeń udanych, nieudanych, aktywnych, łączny rozmiar odtworzonych danych), • zbiorcze procentowe zestawienie udanych zadań kopii bezpieczeństwa z poszczególnych serwerów, • zbiorcze zestawienie zabezpieczanych serwerów które w sposób ciągły (kilka razy pod rząd) miały błędy z wykonaniem kopii bezpieczeństwa, • zestawienie ewidencjonowanych wirtualnych maszyn, które nie podlegają procesom realizacji kopii bezpieczeństwa, • spodziewany czas odtwarzania zabezpieczanego serwera oraz potencjalnej utraty danych (czas między ostatnią kopią bezpieczeństwa a chwilą awarii), • najmniej wiarygodne zabezpieczanych serwery (procent nieudanych procesów kopii bezpieczeństwa), • lista najwolniejszych/najszybszych zabezpieczanych maszyn, • poziom SLA (procentowa liczba udanych zadań kopii bezpieczeństwa) w odniesieniu do poziomu założonego, • mierzenie poziomu SLA dla poszczególnych zabezpieczanych serwerów przy uwzględnieniu założonego okna backupowego i RPO (punktu do którego się odtwarzamy), • liczba danych zabezpieczanych dziennie, • liczba zadań realizacji kopii bezpieczeństwa dziennie, • zużycie zasobów na serwerach zarządzających procesami kopii bezpieczeństwa (procesor, pamięć, karty sieciowe LAN, SAN), • zużycie mediów składujących kopie i napędów taśmowych, • aktualna konfiguracja systemu zarządzającego procesami kopii bezpieczeństwa, • historia zmian konfiguracji systemu zarządzającego procesami kopii bezpieczeństwa,

28.	W ramach dostarczonych licencji musi istnieć możliwość zaindeksowania oraz przeszukiwania kopii bezpieczeństwa z poziomu graficznego interfejsu (GUI), wymagana także możliwość wyszukania dowolnych fraz w nazwach plików.
29.	Musi istnieć możliwość zabezpieczenia dowolnej maszyny wirtualnej wraz z aplikacjami w trybie ciągłym tzn. umożliwiającym odtworzenie do dowolnego punktu w czasie (tzw. PIT – Point In Time), wymagane wsparcie dla VMware ESXi 6,7 i 7.
30.	Oprogramowanie musi posiadać wsparcie dla replikacji (bi-directional) asynchronicznej oraz synchronicznej (realizowanej na poziomie dostarczanego oprogramowania), połączonych z mechanizmem tzw. JOURNALING umożliwiającego odnotowanie wszystkich zmian zabezpieczanego środowiska
31.	Oprogramowanie musi posiadać wsparcie dla równoległej replikacji zabezpieczanego środowiska do różnych ośrodków docelowych (min. 3-ech), wsparcie dla replikacji równoległej powinno być zapewnione również na poziomie grup wirtualnych maszyn (tzw. CONSISTENCY GROUP)
32.	Oferowane oprogramowanie musi umożliwiać: • stworzenia DISASTER RECOVERY dla całego zabezpieczanego wirtualnego środowiska zbudowanego w oparciu o VMware vSphere, • operacyjne ODTWARZANIE dowolnej maszyny VM wraz z aplikacjami, • MIGRACJI danych w trybie ON-LINE na inne zasoby dyskowe.
33.	Oprogramowanie musi posiadać równoległe wsparcie środowisk lokalnych oraz zdalnych, wymagana możliwość pracy w 3-ech trybach, tzw.: CDP (Continuous Data Protection - tryb replikacji lokalnej), CRR (Continuous Remote Replication - tryb replikacji zdalnej), CLR (Continuous Local and Remote Replication, połączenie CDP oraz CLR - tryb replikacji lokalnej oraz zdalnej) w ramach dostarczonych licencji.
34.	Oprogramowanie musi posiadać granularność umożliwiającą pominięcie określonych plików VMDK związanych z wirtualnymi maszynami objętymi ochroną
35.	Wyskalowanie systemu powinno gwarantować RPO (Recovery Point Objective) w przypadku codziennej pracy ciągłej na poziomie pojedynczych sekund
36.	System musi zapewnić następującą retencję przechowywanych kopii bezpieczeństwa: • RPO=30s z ostatnich 24h, • RPO=24h z ostatniego tygodnia, • RPO=1tydzień z ostatniego miesiąca.
37.	Oprogramowanie musi posiadać możliwość odtworzenia zabezpieczanego środowiska do DOWOLNEGO punktu w czasie w zakresie objętym mechanizmem tzw. JOURNALINGu
38.	Oprogramowanie musi posiadać możliwość trybu pracy umożliwiającego objęciem protekcją w sposób automatyczny nowo dodanych maszyn wirtualnych (VM)
39.	Oprogramowanie, w przypadku wirtualnych maszyn z zainstalowanym systemem operacyjnym Windows Server, musi posiadać wsparcie dla VSS oraz zapewnienie konsystencji aplikacji na poziomie VSS
40.	Oprogramowanie musi posiadać możliwość automatycznego przeprowadzania operacji typu FAILOVER/FAILBACK do dowolnego punktu w czasie dla określonych produkcyjnych serwerów wirtualnych (VM), w tym: odtworzenie, uruchomienie (z zachowaniem wymaganej sekwencji) w zakresie objętym mechanizmem tzw. JOURNALINGu,
41.	Oprogramowani musi posiadać możliwość automatycznego zainicjowania procesu REVERSE REPLICATION w przypadku procesów FAILOVER/FAILBACK
42.	Wymagane jest dostarczenie licencji zapewniających funkcjonalność: ENCRYPTION (szyfrowanie) w obrębie maksymalnej wymaganej pojemności urządzenia.
43.	Musi istnieć możliwość uruchomienia zdalnych konsol dla:

	• aplikacji zarządzających procesem realizacji kopii bezpieczeństwa • systemu dedykowanego do raportowania • systemu dedykowanego do przeszukiwania danych kopii bezpieczeństwa • systemu CDP stworzonych w oparciu o oprogramowanie będące przedmiotem zapytania, możliwość zdalnego uruchomienia oraz wyłączenia w/w komponentów
44.	Zapewnienie podglądu on-line takich elementów jak: • aktywność procesów realizujących kopie bezpieczeństwa • aktywność procesów replikacyjnych • aktualny status • alarmy
45.	Możliwość zarządzania procesem wyszukiwania danych kopii bezpieczeństwa

3. Usługi

Serwer kopii bezpieczeństwa:

- instalacja i konfiguracja serwera: w tym montaż w szafach RACK, podłączenie zasilania, sieci management, synchronizacja czasu NTP, aktualizacja oprogramowania układowego i jego komponentów do rekomendowanych przez producenta wersji, konfiguracja uprawnień użytkowników oraz uruchomienie i sprawdzenie poprawności działania.
- podłączenie i wdrożenie serwera do pracy w infrastrukturze Zamawiającego,
- skonfigurowanie replikacji magazynów danych z deduplikacją pomiędzy urządzeniami,
- wdrożenie do działania oprogramowania systemowego do realizacji kopii bezpieczeństwa w najnowszych rekomendowanych przez producenta wersjach, w tym przede wszystkim komponentów oprogramowania zarządzającego procesem zapisu kopii bezpieczeństwa na warstwę przestrzeni zrealizowaną na taśmach,
- rekonfiguracja posiadanych przez Zamawiającego urządzeń Dell EMC DataDomain 6300 w zakresie przeznaczenia ich do pełnienia roli celu dla mechanizmów replikacji i/lub klonowania kopii bezpieczeństwa,
- przeprowadzenie testów akceptacyjnych poprawności działania operacji wykonywania kopii bezpieczeństwa i odzyskiwania danych zarówno z serwera, replik danych kopii bezpieczeństwa na urządzeniach Zamawiającego, jak i z nośników taśmowych (modułu archiwizującego),
- rekonfiguracja środowiska wirtualizacji opartego o oprogramowanie VMware vSphere w zakresie umożliwiającym wykonywanie kopii bezpieczeństwa przez dostarczone rozwiązanie,
- implementacja kont użytkowników i polityki dostępu do serwera kopii bezpieczeństwa,
- integracja dostarczanych rozwiązań i oprogramowania z posiadanym przez Zamawiającego oprogramowaniem kopii bezpieczeństwa,
- wykonanie testów komunikacji pomiędzy klientami i serwerem oraz pomiędzy klientami i serwerami deduplikacji posiadanymi przez Zamawiającego,
- konfiguracja i implementacja wskazanej przez Zamawiającego polityki kopii bezpieczeństwa wraz z uwzględnieniem archiwizacji kopii na taśmy, przy uwzględnieniu zatrzymania obecnych polis,
- przeprowadzenie testów akceptacyjnych polegających na weryfikacji poprawności backupu i odtwarzania wirtualnych maszyn, z wykorzystaniem dostarczanego serwera

kopii bezpieczeństwa, jak i posiadanych przez Zamawiającego serwerów z deduplikacją oraz z archiwum na taśmach.

4. Przygotowanie dokumentacji powykonawczej przedmiotu zamówienia.

Dokumentacja musi zawierać co najmniej informacje o:

- Architekturze logicznej w zakresie implementacji rozwiązania,
- Architekturze fizycznej w zakresie implementacji rozwiązania,
- Architekturze sieciowej w zakresie implementacji rozwiązania,
- Konfiguracji serwera kopii bezpieczeństwa - zarówno dostarczanego, jak i w zakresie elementów systemu posiadanego przez Zamawiającego.