OPIS PRZEDMIOTU ZAMÓWIENIA

Spis pozycji

1) Wdrożenie systemu backupu danych i archiwizacji danych z replikacją (zakup sprzętu) - Klaster serwerów – 2 szt.

W skład każdego z klastra wchodzi:

a) Zintegrowany serwer do backupu danych (do każdego klastra)

L.p.	**Minimalne wymagania i funkcjonalności** *(zintegrowany serwer do backupu danych)*
1.	Urządzenie musi być gotowym produktem pochodzącym od jednego producenta, musi być oznaczony nazwą i typem dostępnym w katalogu produktów określonego producenta, obecnie oferowanym przez producenta na rynku. Musi umożliwiać: - tworzenie kopii zapasowych (backupu) poprzez wykorzystanie deduplikacji na źródle - wykorzystanie medium backupowego dedykowanego do przechowywania zabezpieczanych danych, gwarantującego globalną deduplikację danych - indeksowanie oraz pełnotekstowe przeszukiwanie danych backupowych poprzez wbudowany system - raportowanie w oparciu o wbudowany system.
2.	Urządzenie musi być gotowe do pracy, co oznacza: - wyeliminowanie konieczności instalacji serwera backupowego - wyeliminowanie konieczności instalacji media serwerów - dostarczone urządzenie musi być optymalne pod kątem pracy ciągłej co oznacza wyeliminowanie konieczności strojenia, weryfikacji/zmian konfiguracji oraz przeprowadzania testów strojeniowych
3.	Minimum 5 lat gwarancji producenta realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia. Możliwość zgłaszania awarii w trybie 24x7x365 poprzez linię telefoniczną producenta lub dedykowaną stronę www producenta. Producent gwarancyjnie odpowiada za poprawność pracy całości rozwiązania, czyli za zaimplementowane oprogramowanie systemowe (SW) oraz sprzęt (HW), co w szczególności oznacza: - tworzenie/bezpłatne udostępnianie do pobrania poprawek oprogramowania oraz nowych wersji SW - dedykowanie odpowiednich wersji oprogramowania systemowego rekomendowanego dla eksploatowanej części SW - gwarancję optymalnej pracy całości dostarczonego rozwiązania (niedopuszczalny jest scenariusz w przypadku którego wewnętrzna przyczyna problemu powodującego nieprawidłowe zachowanie dostarczonego rozwiązania, określana jest jako zależna od pracy elementu w przypadku którego producent rozwiązania nie ponosi odpowiedzialności) - producent dostarczonego rozwiązania gwarantuje min. 5-o letnie utrzymanie eksploatacyjne całości rozwiązania wliczając w to SW oraz HW
4.	Serwer musi dysponować przestrzenią netto minimum 48TB przeznaczoną na gromadzenie deduplikatów.
5.	Urządzenie wyposażone w redundantne dwa zasilacze min. 1100 W (230V) oraz zasilacz awaryjny: tzn. UPS-a min. 3000VA, 8xIEC C13+1xIEC C19, technologia online

	(podwójna konwersja), z kartą SNMP oraz dodatkowym modułem bateryjnym min. 72V, montaż w szafie rackowej, gwarancja producenta na UPS-a min. 3 lata.
6.	Urządzenie dedykowane do montażu w szafie rackowej.
7.	Zastosowany w serwerze algorytm deduplikacji powinien bazować na bloku o zmiennej długości, dobieranej automatycznie dla kolejnych zapisywanych na urządzeniu danych. W celu osiągnięcia dużej efektywności deduplikacji maksymalna wielkość bloku wykorzystywanego w tym procesie nie powinna być większa niż 16 kB. Niedopuszczalna jest deduplikacja stałym blokiem o ustalonej tej samej długości, możliwość manulanej zmiany (bądź poprzez oskryptowanie) długości bloku deduplikacji również nie może zastąpić wymogu automatycznego doboru długości bloku na jaki dzielony jest każdy strumień danych.
8.	Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo skompresowane
9.	Tryb zapisu zabezpieczanych danych nie powinien umożliwiać nadpisywania danych, dane mogą być zapisywane jedynie w trybie append-only, dane dla których wygasła retencja powinny zostać usunięte podczas procesu czyszczenia tzw. cleaning.
10.	Wymagane porty służące do komunikacji z oferowanym urządzeniem: min. 8 x Eth 10Gb/s BaseT (w zestawie 8 patchcord-ów RJ45 cat. 6 o długości 3m. każdy w kolorze czerwonym)
11.	Skalowanie urządzenia powinno zapewnić możliwość zwiększenia pojemności netto przeznaczonej do gromadzenia deduplikatów do min. 90TB netto.
12.	Osiągana wydajność zapisu danych w przypadku maksymalnej konfiguracji oferowanego urządzenia deklarowana w ogólnie dostępnej dokumentacji nie powinna być niższa niż 8TB/h.
13.	Możliwość równocześnie (równolegle) wykorzystywanych strumieni nie powinna być mniejsza niż 60.
14.	Przestrzeń dyskowa dedykowana do gromadzenia deduplikatów powinna być zabezpieczona poprzez wykorzystanie RAID 6 i odporna na jednoczesną awarię dwóch dysków.
15.	Oferowane rozwiązanie musi być dedykowane do montażu w szafie RACK, zajętość całości oferowanego rozwiązania z uwzględnieniem skalowania do wymaganej pojemości nie może zajmować więcej niż 2U.

16.	Wymagane oficjalne wsparcie dla systemów:
	- MS Windows Server: 2016, 2012
	- Linux (x64):
	  ○ Red Hat Enterprise Linux: 7.0 … 7.4
	  ○ Suse Enterprise Server: 10 … 12
	  ○ Debian: 6.x … 9.x
	- Unix:
	  ○ IBM AIX (POWER): 7.1, 7.2
	- w przypadku Desktop/Laptop:
	  ○ Windows: Vista, 2008, 2012, 2016, 10
	  ○ Apple OS-X: 10.x
	  ○ Red Hat: 6, 7
	  ○ SuSe: 11, 12
	  ○ Ubuntu: 13.x, 14.x

17.	Wymagane oficjalne wsparcie dla następujących baz danych, w postaci oficjalnie

	dostępnego dedykowanego agenta umożliwiającego realizację konsystentnego backupu on-line: - ORACLE: 11, 12 - MS SQL: 2014, 2016, 2017 - Sharepoint: 2010, 2013, 2016 - Exchange: 2010, 2013, 2016 - DB2: 10.x, 11.x
18.	Wymagana możliwość realizacji backupu wspieranych baz danych w sposób zrównoleglony, wykorzystujący wiele strumieni jednocześnie (min. 10) do backupu poj. bazy danych.
19.	Oferowane urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia), co najmniej następujące aplikacje: RMAN, Microsoft SQL Server Management Studio, IBM Data Studio, SAP BR*Tools, SAP HANA Sudio W przypadku współpracy z każdą z poniższych aplikacji: • RMAN (dla ORACLE) • Microsoft SQL Server Management Studio (dla Microsoft SQL) • IBM Data Studio (dla DB2) • SAP BR*Tools (dla SAP/ORACLE) • SAP HANA Sudio (dla SAP HANA) urządzenie musi umożliwiać deduplikację na źródle i zapis nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN. Deduplikacja danych odbywa się na dowolnym serwerze posiadającym funkcjonalność: serwera RMAN / serwera SQL/ serwera DB2/ serwera SAP . Deduplikacja w wyżej wymienionych przypadkach musi zapewniać aby z zabezpieczanych serwerów do urządzenia były transmitowane poprzez sieć LAN jedynie fragmenty danych nie znajdujące się dotychczas na urządzeniu.
20.	Wymagane oficjalne wsparcie dla backupu następujących platform: - VMware vSphere: 6.5, 6.7 - MS Hyper-V: 2012R2, 2016 umożliwiające backup obrazów maszyn wirtualnych typu „image” jak i backup typu „guest” przy wykorzystaniu agentów bazodanowych.
21.	Urządzenie musi umożliwiać backup oraz odtwarzanie danych w zdalnych lokalizacjach bez pośrednictwa dodatkowych elementów typu dodatkowy serwer czy mediaserwer oraz bez konieczności obsługi systemu przez personel w zabezpieczanej lokalizacji. System powinien być odporny na: - opóźnienia związane z jakością łącz, na poziomie 100 ms - utratę pakietów związaną z jakością łącz na poziomie 10% - zrywaniem i przerwami w transmisji związanymi z jakością łącz, do 20 min.
22.	Konfiguracja backupów w przypadku zasobów w zdalnych lokalizacjach musi być realizowana z poziomu centralnej konsoli, bez konieczności logowania na zabezpieczany serwer.
23.	W przypadku backupu agentowego (agent systemu plików) oferowane rozwiązanie nie może odczytywać z zabezpieczanej maszyny tych plików, które nie zmieniły się w stosunku do wcześniejszego backupu którego retencja nie wygasła. Odczytowi i deduplikacji muszą podlegać jedynie nowe bądź zmienione pliki w stosunku do wcześniej realizowanej kopii backupowej której retencja nie wygasła.

24.	Każdy backup plikowy określonego zasobu, realizowany przez oferowane rozwiązanie musi być backupem pełnym. Wymaga się aby odtworzenie danych plikowych było pojedynczym procesem identycznym ze sposobem odtwarzania danych z inicjalnego pełnego backupu.
25.	Proces odtwarzania danych w przypadku zdalnej lokalizacji musi być realizowany z poziomu centralnej konsoli bez konieczności logowania na serwer którego zasoby podlegają odtwarzaniu.
26.	W przypadku odtwarzania całego systemu plików Windows/Linux (np.: dysk E:\ w Windows, cały system plików w przypadku Linux), wymaga się aby urządzenie w sposób automatyczny porównało pliki znajdujące się w odtwarzanej kopii backupowej oraz na maszynie której zasoby są odtwarzane i odtworzyło jedynie brakujące pliki. Pliki które znajdują się zarówno w kopii backupowej jak i na maszynie której zasoby są odtwarzane nie powinny być przesyłane na docelową maszynę, przy czym proces porównywania plików nie może wymagać ich pełnego odczytywania z urządzenia przechowującego kopie backupowe.
27.	Unikalne bloki (w aspekcie danych przechowywanych na urządzeniu) z zabezpieczanych serwerów przesyłane do oferowanego urządzenia muszą być kompresowane oraz szyfrowane w oparciu o algorytm posługujący się 256-bitowym kluczem.
28.	Wymagana autentyfikacja komunikacji między klientem a serwerem backupu oparta na certyfikatach.
29.	Wewnętrzny sposób licencjonowania nie może wprowadzać ograniczeń co do: - ilości zabezpieczanych maszyn fizycznych oraz wirtualnych - ilości zabezpieczanych laptopów, desktopów - ilości zabezpieczanych zdalnych lokalizacji/oddziałów - rozmiaru backupowanego wolumenu danych, jedynym ograniczeniem może być możliwość pomieszczenia zdeduplikowanych danych na wewnętrznej przestrzeni oferowanego rozwiazania - ilości zabezpieczanych baz danych w trybie on-line, przy wykorzystaniu dedykowanych agentów bazodanowych
30.	W przypadku backupu zdeduplikowanych przez Windows 2012 danych, system musi umożliwiać zabezpieczanie tych danych bez konieczności przywracania ich do postaci oryginalnej (niezdeduplikowanej).
31.	Urządzenie powinno umożliwiać zdefiniowanie limitów wielkości zabezpieczanych zasobów, w przypadku ich przekroczenia dane nie powinny zostać zapisane na oferowanym urządzeniu.
32.	W przypadku środowisk VMware vSphere, oferowane urządzenie musi umożliwiać następujące typy backupu: - backup całych maszyn wirtualnych - backup pojedynczych, wybranych dysków maszyny wirtualnej vmdk - w przypadku backupu zasobów dyskowych, odczytowi z zabezpieczanego systemu muszą podlegać jedynie zmienione bloki maszyn wirtualnych (wymagane wykorzystanie mechanizmu CBT systemu VMware vSphere) - backupy obrazów maszyn wirtualnych muszą być wykonywane przy pomocy technologii CBT systemu VMware vSphere , do oferowanego urządzenia muszą być transferowane jedynie zmienione/nowe bloki, od strony zaoferowanego systemu musza to być backupy pełne. - wymagana możliwość zastosowania wyrażeń regularnych w celu określenia

	które wirtualne dyski VMware vSphere mają być zabezpieczane
33.	W przypadku środowisk VMware vSphere, oferowane urządzenie musi umożliwiać następujący sposób odtwarzania danych: - całych obrazów maszyn wirtualnych - poj. dysków maszyny wirtualnej z backupu całej maszyny wirtualnej
34.	W przypadku środowisk VMware vSphere, oferowane urządzenie musi umożliwiać następujący sposób odtwarzania danych: - odtworzenie całych maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMware vSphere – odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu którego retencja nie wygasła - odtworzenie pojedynczych dysków maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMware vSphere – odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu którego retencja nie wygasła - odtworzenie pojedynczych plików z backupu obrazu maszyny wirtualnej bez konieczności odtworzenia całej maszyny wirtualnej, funkcjonalność musi być dostępna dla obrazów maszyn wirtualnych z zainstalowanym systemem operacyjnym Windows oraz Linux.
35.	W przypadku środowisk VMware vSphere, oferowane urządzenie musi umożliwiać uruchomienie zabezpieczonej maszyny wirtualnej bezpośrednio z medium backupowego przy wykorzystaniu danych backupowych bez konieczności ich odtwarzania (Instant Access). Wymagane oficjalne potwierdzenie (dostępne w dokumentacji) możliwości jednoczesnego uruchomienia 30 maszyn wirtualnych w trybie Instant Access.
36.	W przypadku środowisk VMware vSphere, oferowane urządzenie musi umożliwiać realizację backupu / odtworzenia w trybie „image backup” (backup plików vmdk) maszyn wirtualnych znajdujących się na serwerach VMware ESX bez udziału vCenter.
37.	W przypadku środowisk VMware vSphere, oferowane rozwiązanie musi umożliwiać prezentację (bez konieczności odtworzenia) zbackupowanych obrazów maszyn wirtualnych jako katalogi, w celu umożliwienia ich przeszukiwania po nazwach lub zawartości plików.
38.	W przypadku środowisk VMware vSphere, oferowane rozwiązanie musi umożliwiać automatyczną weryfikację zbackupowanych maszyn wirtualnych. Wymagana możliwość ustalenia harmonogramu zgodnego z kalendarzem weryfikacji maszyn wirtualnych, która powinna zapewniać: - odtworzenie maszyny wirtualnej na zdefiniowanym DataCenter / Data Store - weryfikację podstawowych procesów - możliwość dołączenia skryptu weryfikującego wybrane elementy maszyny wirtualnej - dostępność informacji w konsoli systemu backupu o poprawnej / niepoprawnej weryfikacji maszyny wirtualnej
39.	W przypadku środowisk VMware vSphere wymaga się aby właściciel maszyny wirtualnej posiadał możliwość samodzielnego (bez konieczności kontaktu z administratorem backupu czy tez administratorem VMware) odtworzenia pojedynczych plików z dowolnego backupu obrazu jego maszyny wirtualnej.
40.	W przypadku środowisk VMware vSphere, oferowane rozwiązanie musi zapewniać na zdefiniowanie automatycznych polityk backupowych dla

	- Folderu - Resource Pool oznacza to, że dodanie maszyny wirtualnej do Folderu, czy Resource Pool spowoduje automatyczne zbackupowanie dodanej maszyny wirtualnej zgodnie z polityka zdefiniowana dla Folderu czy Resource Pool.
41.	W przypadku środowisk VMware vSphere, oferowane rozwiązanie musi umożliwiać automatyczne rozpoznawanie nowo utworzonych maszyn wirtualnych i przypisać je do odpowiednich politykach backupowych. Wymagana możliwość konfiguracji następującego scenariusza: - wszystkie nowo utworzone maszyny wirtualne zawierające w nazwie frazę „krytyczna” muszą być backupowane automatycznie co godzinę - wszystkie nowo utworzone maszyny wirtualne zawierające w nazwie frazę „produkcja” muszą być backupowane automatycznie raz w ciągu dnia - pozostałe maszyny wirtualne są backupowane raz na tydzień
42.	W przypadku środowisk VMware vSphere, oferowane rozwiązanie musi umożliwiać automatyczne dodawanie maszyn wirtualnych do odpowiednich polityk backupowych na podstawie: - określonego tekstu zawartego w nazwie zabezpieczanej maszyny - określonego tekstu zawartego w nazwie folderów (wszystkie maszyny których obrazy przechowywane są w tych folderach powinny zostać przypisane do określonej polityki backupowej) - tag’u maszyn wirtualnych zawierających określony tekst - określonego tekstu zawartego w nazwie datastore (wszystkie maszyny których obrazy przechowywane są w tych datastore’ach powinny zostać przypisane do określonej polityki backupowej)
43.	W przypadku środowisk VMware vSphere, oferowane rozwiązanie musi umożliwiać automatyczne usuwanie maszyn wirtualnych z polityk backupowych w tym samym momencie w którym maszyna jest usunięta z vCenter, dotychczasowo wykonane kopie zapasowe takich maszyn muszą być przechowywane zgodnie z założoną wcześniej retencją.
44.	W przypadku środowisk VMware vSphere, oferowane rozwiązanie musi umożliwiać zdefiniowanie polityk backupowych dostępnych dla administratora systemu VMware vSphere z poziomu vCenter. Administrator VMware vSphere musi mieć możliwość przyporządkowania nowo tworzonych maszyn wirtualnych do określonych polityk backupowych.
45.	W przypadku środowisk VMware vSphere, oferowane rozwiązanie musi umożliwiać automatyczną naprawę problemów związanych ze snapshotami. W przypadku gdy VMware vSphere nie usunie snapshotu, oferowane rozwiązanie musi automatycznie ponawiać usunięcie snapshotu a w przypadku konieczności automatycznie konsolidować maszyny wirtualne VMware vSphere.
46.	W przypadku środowisk VMware vSphere, oferowane rozwiązanie musi umożliwiać backup oraz odtworzanie maszyn wirtualnych z poziomu graficznego interfejsu, linii komend oraz poprzez REST API
47.	W przypadku środowisk VMware vSphere oraz backupu obrazów maszyn wirtualnych Windows, oferowane rozwiązanie musi umożliwiać eliminację backupu pliku pagefiles.bin.
48.	W przypadku środowisk VMware vSphere, oferowane rozwiązanie musi umożliwiać automatyczne usuwanie logów bazy MSSQL po backupie obrazu maszyny wirtualnej

	VMware, funkcjonalność ta nie może wymagać instalacji (choćby chwilowej) agenta na maszynie wirtualnej, ani wymagać zainicjowania dodatkowych komend/skryptów.
49.	W przypadku środowisk VMware vSphere oferowane rozwiązanie musi umożliwiać replikację obrazów maszyn wirtualnych do obszaru dostępnego poprzez S3 w AWS. Zreplikowane obrazy muszą umożliwiać szybkie odtworzenie konfiguracji zabezpieczonych maszyn wirtualnych w AWS, mogą również posłużyć jako repozytorium umożliwiające zwrotną replikację tych danych do urządzenia w celu ich lokalnego odtworzenia.
50.	Oferowane urządzenie musi umożliwiać stworzenie warstwy dedykowanej do długoterminowego przechowywania danych w środowiskach typu CLOUD wymagane oficjalne wsparcie dla AWS, MICROSOFT AZURE, GOOGLE CLOUD PLATFORM, ALIBABA CLOUD. Zgodnie ze stworzoną polityką, dane przeznaczone do długoterminowego przechowywania danych powinny zostać automatycznie bezpośrednio (bez udziału dodatkowych elementów HW/SW) migrowane w postaci deduplikatów do przestrzeni zaalokowanej przez urządzenie w środowisku CLOUD, wymagane skalowanie do 190TB netto części CLOUD.
51.	W przypadku środowisk MS Hyper-V, oferowane rozwiązanie musi umożliwiać: - backup pojedynczych plików i baz danych ze środka maszyny wirtualnej - backup całych maszyn wirtualnych (czyli plików VHD reprezentujących wirtualną maszynę) - pełen (full) backup całych maszyn wirtualnych Hyper-V (image level) musi odbywać się poprzez odczyt tylko zmienionych bloków dysków VHD - w/w backup całych maszyn wirtualnych dla Windows, musi pozwalać na odtworzenie pojedynczych plików z obrazu maszyny wirtualnej bez konieczności odtworzenia całej maszyny wirtualnej. Dopuszcza się wykonywanie snapshotów vss maszyn wirtualnych i użycie ich w trakcie backupu obrazów maszyn wirtualnych. W/w wymagane metody backupu muszą być wbudowane w oferowany system, działać w pełni automatyczny bez stosowania dodatkowych skryptów.
52.	W przypadku środowisk MS Hyper-V, oferowane rozwiązanie musi zapewniać spójny backup Exchange / MS SQL przy backupie obrazów maszyn wirtualnych.
53.	W przypadku środowisk Windows 2012, 2016 wymagana funkcjonalność Bare Metal Recovery automatycznego odtworzenia całego serwera (system operacyjny + ustawienia systemu operacyjnego + dane) w jednym kroku bezpośrednio z oferowanego urządzenia, funkcjonalność ta musi być wbudowana w oferowane rozwiązanie.

54.	W przypadku odtwarzania danych z interfejsu dostępnego na zabezpieczanym serwerze, oferowane rozwiązanie musi zapewniać mechanizm autentyfikacji użytkowników dostępny w dwóch opcjach:
	- wbudowany w oferowane rozwiązanie
	- zintegrowany z usługami katalogowymi
	- w przypadku wykorzystania AD, użytkownicy będący w domenie nie muszą się logować do systemu backupu w przypadku konieczności
	  ○ odtworzenia danych
	  ○ przeszukania zawartości swoich backupów
	  ○ wykonania backupu

55.	W przypadku odtwarzania danych z interfejsu końcowego użytkownika dostępnego na zabezpieczanym laptopie / PC oferowane rozwiązanie musi zapewniać następujące

	funkcjonalności:
	- możliwość wyszukiwania pliku do odtwarzania po
	  o nazwie pliku
	  o początkowym fragmencie nazwy pliku
	  o końcowym fragmencie nazwy pliku
	  o fragmencie nazwy pliku umiejscowionym gdziekolwiek w pełnej nazwie pliku
	- możliwość przeglądania zawartości zabezpieczonego systemu plików i wybór zasobów do odtworzenia
	- wybór wersji odtwarzanego pliku / katalogu

56.	Oferowane rozwiązanie musi mieć możliwość instalacji agentów jako plików msi, wymagana możliwość automatyzacji instalacji agentów poprzez wykorzystanie skryptu przyporządkowującego zabezpieczaną maszynę do określonej polityki backupowej, wymagana możliwość automatycznej aktualizacji oprogramowania agentów.
57.	Oferowane rozwiązanie musi mieć możliwość definiowania ważności przechowywanych backupów na podstawie kryteriów czasowych (dni, miesiące, lata). Po okresie ważności backupy musza być automatycznie usunięte.
58.	Oferowane rozwiązanie musi mieć możliwość tworzenia z poziomu GUI (konsoli graficznej) polityk retencyjnych typu „dziadek – ojciec – syn”, to znaczy utworzenia polityki w której zdefiniowano: - czas przechowywania backupów dziennych - czas przechowywania backupów tygodniowych - czas przechowywania backupów miesięcznych - czas przechowywania backupów rocznych
59.	Oferowane rozwiązanie musi umożliwiać tworzenie wykluczeń, czyli elementów nie podlegających backupowi w ramach zadania backupowego, wymagana możliwość wykluczeń dla dowolnej kombinacji następujących elementów: - wybranych typów plików, (np.: .mp3) - dla całych katalogów (np.: c:\windows). - dla pojedynczych plików
60.	Oferowane rozwiązanie musi umożliwiać realizację backupu typu NDMP serwerów NAS z następującymi funkcjonalnościami: - w trakcie backupu z systemu NAS muszą być wysyłane do medium backupowego tylko nowe/zmienione pliki od ostatniego backupu którego retencja nie wygasła - w przypadku odtwarzania, uprawnienia użytkowników również są odtwarzane - odtworzenie plików z backupu NDMP bezpośrednio na platformę Windows/Linux
61.	Oferowane rozwiązanie musi posiadać możliwość monitorowania, raportowania oraz analizy błędów dla środowiska kopii zapasowej, wymagana dostępność następujących raportów: - podsumowanie zadań backupowych (liczba backupów udanych, nieudanych, aktywnych, łączny rozmiar zbackupowanych danych) - podsumowanie zadań odtworzeniowych (liczba odtworzeń udanych, nieudanych, aktywnych, łączny rozmiar odtworzonych danych danych) - zbiorcze procentowe zestawienie udanych zadań backupowych z

	poszczególnych serwerów - zbiorcze zestawienie zabezpieczanych serwerów w przypadku których kilka razy pod rząd wystąpił problem związany z realizacją backupu - zestawienie zabezpieczanych systemów plików które nie są backupowane - spodziewany czas odtworzenia zabezpieczanego serwera oraz potencjalnej utraty danych (czas między ostatnim backupem a chwilą awarii) - lista najwolniej/najszybciej zabezpieczanych maszyn - poziom SLA (procentowa liczba udanych backupów) w odniesieniu do poziomu założonego - poziom SLA dla poszczególnych zabezpieczanych serwerów przy uwzględnieniu założonego okna backupowego i RPO - ilość dziennych danych backupowych - ilość dziennych zadań backupowych - aktualna konfiguracja systemu backupowego - historia zmian konfiguracji systemu backupowego - posiadane licencje systemu backupowego - wykorzystanie systemu backupowego przez poszczególne grupy użytkowników (chargeback per cost center)
62.	Wymaga się aby oferowane urządzenie umożliwiało zaindeksowania oraz przeszukiwania backupów z poziomu graficznego interface'u (GUI), wymagana również możliwość wyszukania dowolnych fraz w nazwach plików.
63.	Wymaga się aby oferowane urządzenie umożliwiało bezpośredni zapis danych z systemów LINUX oraz WINDOWS z wykorzystaniem deduplikacji na źródle bez jakichkolwiek limitów licencyjnych oraz dodatkowych kosztów (wybrany zasób urządzenia powinien być widoczny od strony systemu LINUX oraz WINDOWS jak zasób dyskowy.
64.	Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych (bez pośrednictwa dodatkowych modułów) do drugiego urządzenia tego samego typu oraz, wymagane następujące tryby pracy replikacji: • jeden do jednego • wiele do jednego • jeden do wielu • kaskadowej (urządzenie A replikuje dane do urządzenia B które te same dane replikuje do urządzenia C). Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu, rozwiązanie replikacyjne nie może wymagać aby obszar na który dane są replikowane był większy od obszaru źródłowego (replikowanego) w przypadku schematu „jeden do jednego" – weryfikacja na podstawie ogólnie dostępnej dokumentacji producenta oraz zaleceń. Ewentualna licencja na replikację musi być dostarczona w ramach postępowania.
65.	W przypadku replikacji danych między dwoma urządzeniami kontrolowanej przez systemy: oferowaną aplikację backupową/ VERITAS NetBackup /EMC NetWorker muszą być możliwe do uzyskania jednocześnie wszystkie następujące funkcjonalności: • replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących • replikacji podlegają tylko te fragmenty danych, które nie znajdują się na

	docelowym urządzeniu replikacja zarządzana jest z poziomu aplikacji backupowej, aplikacja backupowa posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach bez konieczności przeprowadzania procesu inwentaryzacji
66.	W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami.
67.	Narzut na wydajność związany z replikacją nie może zmniejszyć wydajności urządzenia o więcej niż 10%.
68.	Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami.

b) Serwer do archiwizacji danych (do każdego klastra)

Parametr	Charakterystyka i minimalne wymagania *(serwer do archiwizacji danych)*
Obudowa	Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów NFC/ BLE/ WIFI.
Płyta główna	Płyta główna z możliwością zainstalowania minimum jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych
Procesor	Zainstalowany jeden procesor, min. 32-rdzeniowy klasy x86, z 256MB pamięci Cache, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 221 punktów w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org. Możliwość zainstalowania procesora 64-rdzeniowego.
RAM	Minimum 512GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 2TB pamięci RAM.
Zabezpieczenia pamięci RAM	Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling
Gniazda PCI	- minimum 1 slot x16 generacji 3 oraz min. 1 slot x16 generacji 4 połowy wysokości.
Interfejsy	Wbudowane min. dwa interfejsy sieciowe 1Gb Ethernet w standardzie

sieciowe/FC/SAS	BaseT. Dodatkowa karta dwuportowa 10GbE BaseT oraz jedna karta dwuportowa HBA FC 16Gb.
Dyski twarde	Możliwość instalacji dysków SATA, SAS, SSD, NVMe. Zainstalowane min. 8 dysków SAS 2.4TB 10K RPM, 12Gb/s 2,5“ Hot-Plug. Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 240GB z możliwością konfiguracji w RAID 1. Zainstalowany dedykowany moduł dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 32GB. Rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający min. 2GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfujących
Wbudowane porty	min. 1 port USB 2.0, 1 port micro USB oraz 3 porty USB 3.0, 2 porty RJ45, 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym), min. 1 port RS232
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1680x1050
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug min. 550W każdy.
Bezpieczeństwo	Zintegrowany moduł TPM min. 1.2 Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
Diagnostyka	Możliwość instalacji panelu LCD umieszczonego na froncie obudowy, umożliwiającego wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika • możliwość podmontowania zdalnych wirtualnych napędów • wirtualną konsolę z dostępem do myszy, klawiatury • wsparcie dla IPv6 • wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer • integracja z Active Directory • możliwość obsługi przez ośmiu administratorów jednocześnie • Wsparcie dla automatycznej rejestracji DNS • wsparcie dla LLDP

	• wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej • możliwość podłączenia lokalnego poprzez złącze RS-232. • możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy. • Monitorowanie zużycia dysków SSD • możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi, • Automatyczne zgłaszanie alertów do centrum serwisowego producenta • Automatyczne update firmware dla wszystkich komponentów serwera • Możliwość przywrócenia poprzednich wersji firmware • Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON • Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych • Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001. Serwer musi posiadać deklarację CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows 2012, Microsoft Windows 2012 R2 x64, Microsoft Windows 2016, Microsoft Windows 2019 (wydruk ze strony).
Warunki gwarancji	Minimum 5 lat gwarancji producenta realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia. Możliwość zgłaszania awarii w trybie 24x7x365 poprzez linię telefoniczną producenta/wykonawcy lub dedykowaną stronę www producenta/wykonawcy. Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. W okresie gwarancji uszkodzone dyski pozostają w siedzibie Zamawiającego.
Dokumentacja użytkownika	Wymagana dokumentacja w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

2) Wdrożenie systemu backupu danych i archiwizacji danych z replikacją

a) Rozbudowa obecnej przestrzeni do archiwizacji danych

Doposażenie istniejącej macierzy DELL/EMC SCv3020 o numerze Service Tag 4T0Q2T2 będącej własnością Zamawiającego w 13 dysków (w 13 wolnych zatok macierzy).

Dyski o pojemności minimum 1.2TB SAS, prędkości 10k RPM, wielkość 2.5" pochodzące w oficjalnego kanału dystrybucji producenta, fabrycznie nowe, pochodzące z bieżącej produkcji.

b) Rozwiązanie do wirtualizacji serwerów do archiwizacji danych

System do wirtualizacji musi spełniać:

1. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych
2. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
3. Pojedynczy klaster może się skalować do 64 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji.
4. Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć i wykorzystać procesory fizyczne wyposażone w 576 logicznych wątków oraz do 12 TB pamięci fizycznej RAM.
5. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych.
6. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB.
7. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych
   z możliwością przydzielenia do 6 TB pamięci operacyjnej RAM.
8. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych.
9. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe.
10. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
11. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.

12. Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). Licencjonowanie nie może odbywać się w trybie OEM.
13. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows XP, Windows Vista, Windows 2000, Windows Server 2003/R2, Windows Server 2008/R2, Windows Server 2012/R2, Windows Server 2016, Windows 7, Windows 8, Windows 8.1, Windows 10, SUSE Linux Enterprise Server, Red Hat Enterprise Linux, Solaris, Oracle Enterprise Linux, Debian GNU/Linux, CentOS, FreeBSD, Asianux, NeoKylin Linux, CoreOS, Ubuntu, SCO OpenServer, SCO Unixware, Mac OS X.
14. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
15. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
16. Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania zarówno jako aplikacja na maszynie fizycznej lub wirtualnej, jak i jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance. Dostęp do konsoli może być realizowany z poziomu przeglądarki internetowej z wykorzystaniem protokołu HTML5.
17. Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku.
18. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
19. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
20. Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
21. Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn. Mechanizm ten jest elementem składowym rozwiązania i nie wymaga dodatkowej licencji na system operacyjny.
22. Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych.
23. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie.

24. Rozwiązanie musi mieć możliwość przenoszenia zwirtualizowanych dysków maszyn wirtualnych w czasie ich pracy pomiędzy fizycznymi zasobami dyskowymi. Mechanizm powinien umożliwiać realizację co najmniej 2 takich procesów przenoszenia jednocześnie.
25. Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA) , aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym.
26. Oprogramowanie do wirtualizacji musi zapewniać mechanizm takiego zabezpieczenia wybranych przez administratora wirtualnych maszyn, aby w przypadku awarii lub niedostępności serwera fizycznego maszyny, które na nim pracowały, były bezprzerwowo dostępne na innym serwerze z zainstalowanym oprogramowaniem wirtualizacyjnym. Mechanizm ten umożliwia zabezpieczenie maszyn wirtualnych wyposażonych w minimum 2 wirtualne procesory.
27. System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów.
28. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
29. Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN).
30. Oprogramowanie musi posiadać minimum 5 lat subskrypcji.
31. Oprogramowanie musi obejmować 6 licencji (oprogramowanie licencjonowane per CPU) – oprogramowanie nie może być ograniczone do obsługi hostów 2 procesorowych, Zamawiający wymaga aby licencje dostarczone w tym postępowaniu pozwalały na objęcie licencją również hostów 1 procesorowych oraz 4 procesorowych.
32. Zamawiający dopuszcza licencje edukacyjne.
33. Oprogramowanie musi posiadać centralną konsolę graficzną do zarządzania wieloma maszynami wirtualnymi oraz ich zasobami pracującymi na wielu serwerach fizycznych umożliwiając:
    - globalne zarządzanie kontrolą dostępu do serwerów i maszyn wirtualnych,
    - wykonywanie automatycznych bądź manualnych zadań w celu optymalizacji infrastruktury dla maszyn wirtualnych,
    - widok całego systemu i zbioru maszyn wirtualnych. Mapy Infrastruktury,
    - możliwość monitorowania dostępności i wydajności maszyn wirtualnych,
    - możliwość raportowania dostępności i wydajności maszyn wirtualnych,
    - funkcje ochrony dostępu zintegrowane z mechanizmem uwierzytelniania Windows,
    - planowanie zadań i ustawianie znaczników alarmów w celu generowania automatycznych powiadomień o statusie serwerów lub maszyn wirtualnych,
    - tworzenie obrazów maszyn wirtualnych,
    - klonowanie maszyn wirtualnych,

- wykonywanie wielu kopii migawkowych (snapshot) w każdym momencie pracy maszyny wirtualnej oraz możliwość powrotu do jej stanu z każdego momentu zrobienia kopii.

c) Rozbudowa infrastruktury sieciowej w celu podłączenia klastrów serwerowych

Doposażenie dwóch przełączników sieciowych posiadanych przez Zamawiającego (DELL EMC BROCADE 6505 o numerach seryjnych BRCCCD1934P05J, BRCCCD1934P05E) w 12 modułów FC 16Gb każdy. pochodzących z oficjalnego kanału dystrybucji producenta, fabrycznie nowych, pochodzących z bieżącej produkcji wraz z 12-toma patchcord-ami koloru czerwonego (do każdego przełącznika) o długości 3m. każdy, multimode o złączach LC-LC.

d) Wyposażenie serwerów archiwizacji danych w system operacyjny

W celu wdrożenia systemu do backupu i archiwizacji danych należy doposażyć (dostarczyć) każdy z dwóch serwerów do archiwizacji danych w system operacyjny Red Hat Enterprise Linux Server, Standard (Physical or Virtual Nodes) - 1 physical entitlement for a Server (2-sockets, Stackable) OR 2 Virtual Instances - 5YR lub inny w pełni równoważny komercyjny system operacyjny zapewniający wysoką wydajność i niezawodność, oferujący rozbudowane możliwości wirtualizacji. System z min. 5-letnim prawem dostępu do repozytoriów producenta i aktualizacji systemu. Najnowsza stabilna wersja.

e) Implementacja (wdrożenie) systemu backupu danych i archiwizacji danych w siedzibie Zamawiającego

Wymagania dot. wdrożenia - Implementacja systemu kopii zapasowych:

1. Konfiguracja i montaż urządzeń fizycznych, dedykowanych do zadań serwera kopii zapasowych
2.Podłączenie serwera do sieci LAN/SAN
3.Konfiguracja urządzeń fizycznych:
a. parametryzacja dostępu do interfejsu zarządzania serwerem,
b. konfiguracja lokalnej przestrzeni dyskowej.
4. Aktualizacja mikrokodu (firmware) komponentów serwera do najnowszej zalecanej przez producenta wersji.
5. Instalacja systemu operacyjnego wirtualizatora dla systemu kopiowania i odtwarzania danych
6. Konfiguracja parametrów systemu operacyjnego (LAN), instalacja poprawek systemowych
7. Instalacja dostarczonego systemu kopiowania i odtwarzania danych jako maszyna wirtualna
8. Konfiguracja parametrów sieciowych systemu kopiowania i odtwarzania danych
9. Instalacja dostarczonego systemu składowania kopii zapasowych z funkcją deduplikacji danych jako maszyna wirtualna
10. Konfiguracja parametrów sieciowych systemu deduplikatora
11. Konfiguracja protokołów dostępowych do deduplikatora
12. Konfiguracja urządzeń składowania danych (repozytoria kopii zapasowych):
a. Przestrzenie dyskowe

b. Przestrzenie dyskowe z deduplikacją
13. Organizacja przestrzeni dyskowej na obecnie posiadanych oraz dostępnych zasobach macierzy dyskowych oraz dedykowanie tejże przestrzeni na potrzeby systemu kopii zapasowych
14. Konfiguracja przestrzeni dyskowej dedykowanej dla składowania unikatowych bloków
15.Prezentacja danych dla systemu kopiowania i odtwarzania danych
16.Konfiguracja polityk ochrony dla wskazanych maszyn wirtualnych/fizycznych:
a. Definicje typów kopii zapasowych (obraz maszyny, dane plikowe, dane aplikacyjne w trybie online, dane aplikacyjne w trybie offline)
b. Definicja harmonogramów
c. Definicja miejsc składowania kopii zapasowych
d. Definicja polityk retencji
e. Testy odtwarzania danych
17. Konfiguracja polityk ochrony dla wskazanych 20 stacji roboczych:
a. Definicje typów kopii zapasowych (dane plikowe, dane aplikacyjne w trybie online, dane aplikacyjne w trybie offline)
b. Definicja harmonogramów
c. Definicja miejsc składowania kopii zapasowych
d. Definicja polityk retencji
e. Testy odtwarzania danych
18. Przeszkolenie dla administratorów systemu w wymiarze 8h w siedzibie Zamawiającego.

UWAGA: Oferowany sprzęt i akcesoria, spełniające powyższe wymagania, muszą być fabrycznie nowy i pochodzić z bieżącej produkcji. Wykonawca składając ofertę musi wskazać producenta oraz model oferowanego sprzętu (ogólnie dostępnego w ofercie producenta). Dostawa do siedziby Zamawiającego na koszt Dostawcy/Wykonawcy.