Załącznik nr 1 do SIWZ

Opis Przedmiotu Zamówienia

Rozbudowa systemu kopii bezpieczeństwa poprzez budowę systemu zarządzania kopiami zapasowymi danych

1 Opis przedmiotu zamówienia

Zamawiający wymaga

- dostarczenia systemu do backupu pozwalającego na zabezpieczenie min. 160 wirtualnych maszyn w środowisku VMware ESX wraz z aplikacjami, min. 1 agenta dla backupu serwera Sharepoint zlokalizowanego w usłudze MS365 oraz tworzenia kopii zapasowej min. 100 skrzynek mailowych Exchange w usłudze MS365 z możliwością granularnego odtworzenia.
- wdrożenie dostarczonych rozwiązań
- przeprowadzenia szkolenia z wdrażanego rozwiązania

2 Definicje

- archiwizacja - czynność przeniesienia danych w inne miejsce w pamięci masowej, w celu ich długotrwałego przechowywania
- backup - kopia bezpieczeństwa danych w celu ich odtworzenia po utracie lub uszkodzeniu
- incremental forever - pełna informacja o plikach włączonych do backupu jest przesyłana tylko za pierwszym razem, kolejna jest kopią przyrostową i zawiera jedynie zmiany, które zaszły od ostatniej kopii
- synthetic full – backup powstaje na skutek konsolidacji kopii pełnej i następujących po niej kopii przyrostowych
- System kopii zapasowej – zestaw oprogramowanie i niezbędna infrastruktura sprzętowa do realizacji zadań backupu i archiwizacji
- tryb 5x9xNBD – okno zgłoszeń 9 godzin, 5 dni w tygodniu, 365 dni w roku

3 Lista wymaganych funkcjonalności

3.1 Architektura

3.1.1 Rozwiązanie Systemu kopii zapasowych powinno reprezentować architekturę trójwarstwową (serwer zarządzający, serwer pośredniczący w zapisie/odczycie danych - proxy oraz klient), pozwalającą na elastyczną skalowalność rozwiązania bez względu na wielkość przyrostu danych.

3.1.2 Oprogramowanie Systemu kopii zapasowych nie może preferować żadnej platformy sprzętowej, nie może być profilowane pod konkretnego dostawcę sprzętu serwerowego oraz producenta pamięci masowych. Niedopuszczalne jest, aby funkcjonalności związane z zabezpieczaniem danych były w jakikolwiek sposób związane czy zależne od konkretnego typu czy producenta urządzenia.

3.1.3 Zamawiający zapewni platformę sprzętową do uruchomienia oprogramowania i przechowywania kopii zapasowych

3.1.4 Jeśli System kopii zapasowych korzysta z bazy danych, to wszelkie potrzebne licencje muszą zostać dostarczone i stanowić całość Systemu, z tym, że licencje dla silnika bazodanowego muszą pozwalać na zainstalowanie go na serwerze fizycznym, klastrze active-passive, serwerze wirtualnym w środowisku VMware i Hyper-V

3.1.5 Licencje muszą pozwalać na stworzenie dla serwera zarządzającego rozwiązania wysokodostępnego z czasem przełączenia nie dłuższym niż 15 minut za pomocą funkcji wbudowanych w oprogramowanie. Jeśli do stworzenia takiego rozwiązania potrzebne są licencje replikacyjne, klastrowe, współdzielona przestrzeń dyskowa to muszą być dostarczone i stanowić całość Systemu

3.1.6 Oprogramowanie Systemu kopii zapasowych musi umożliwiać zdalne instalowanie i odinstalowywanie klienta systemu z centralnego serwera dla systemów Windows, Linux i Unix

3.1.7 System kopii zapasowych musi zapewniać funkcjonalność odtwarzania po awarii konfiguracji serwera zarządzającego poprzez tworzenie kopii bezpieczeństwa i archiwów.

3.1.8 System kopii zapasowych musi posiadać możliwość nieodwracalnego kasowania danych – funkcjonalność ta musi być częścią oprogramowania.

3.1.9 Dla dowolnego transferu danych z klienta musi istnieć możliwość definiowania/ograniczania pasma dla transferu danych – funkcjonalność ta musi być dostępna także przy włączonej deduplikacji na kliencie.

3.1.10 System kopii zapasowych musi pozwalać na składowanie danych na taśmach celem przechowywania długoterminowego.

3.1.11 System kopii zapasowych musi pozwalać na zarządzanie całością działania systemu (backup, archiwizacja, backup stacji roboczych) z jednej konsoli administracyjnej.

3.1.12 Dla zarządzania Systemem kopii zapasowych musi być dostępna konsola administracyjna uruchamiana poprzez przeglądarkę internetową (min. Microsoft Edge, Mozilla Firefox, Google Chrome) – w pełni funkcjonalne zarządzanie systemem poprzez interfejs webowy.

3.1.13 Komunikacja agentów Systemu kopii zapasowych z serwerami musi odbywać się poprzez SSL – konfiguracja tego typu transferu nie wymaga instalowania dodatkowego oprogramowania.

3.1.14 System kopii zapasowych musi pozwalać na współdzielenie napędów taśmowych w środowisku sieci SAN.

3.1.15 System kopii zapasowych musi pozwalać na przechowywanie kopii danych na nośnikach taśmowych.

3.2 Deduplikacja

3.2.1 System kopii zapasowych musi posiadać wbudowaną funkcjonalność deduplikacji. Funkcjonalność ta musi działać na poziomie blokowym i być wykonywana online podczas procesu tworzenia kopii danych. Deduplikacja musi być realizowana poprzez oprogramowanie Systemu kopii zapasowych na dowolnym sprzęcie czy to w warstwie serwera systemu czy klienta. Pojedynczy serwer Systemu kopii zapasowych musi umożliwiać przechowywanie minimum 200 TB danych po deduplikacji (rozbudowa do tej wielkości może nastąpić tylko poprzez dodanie dodatkowych dysków czy macierzy dyskowej).

3.2.2 Włączenie funkcjonalności deduplikacji na kliencie musi być możliwe dla różnych systemów operacyjnych: Windows, Linux, Unix i Macintosh.

3.2.3 Włączenie funkcjonalności deduplikacji nie może generować wymogu instalacji dodatkowych modułów programowych po stronie klienckiej lub serwera systemu.

3.2.4 Deduplikacja blokowa musi obejmować dane nie tylko backupowane, ale i archiwizowane, przy czym wielkość bloku nie może być większa niż 128KB.

3.2.5 System kopii zapasowych musi zapewniać wspólny stopień deduplikacji (jedna baza deduplikacyjna) dla danych z backupu i z archiwizacji.

3.2.6 System kopii zapasowych musi umożliwiać wykonywanie kopii w post procesie do drugiej lokalizacji przesyłając jedynie unikalne bloki danych (dla dowolnych danych z procesu: backupu, archiwizacji). Replikacja danych do innej lokalizacji musi być wykonywana na danych po deduplikacji i funkcjonalność ta musi być realizowana i zarządzana z poziomu Systemu kopii zapasowych.

3.2.7 Proces przesyłania danych (replikacji) na inny serwer Systemu kopii zapasowych celem tworzenia dodatkowej kopii danych nie może być zależny od warstwy sprzętowej (dowolny producent serwera, dowolny producent macierzy/półki dyskowej).

3.2.8 System kopii zapasowych musi pozwalać na instalację bazy deduplikacyjnej w układzie wysokiej dostępności (minimum na dwóch serwerach w dwóch lokalizacjach) w taki sposób, aby awaria pojedynczego serwera nie powodowała utraty możliwości deduplikacji i odtwarzania danych.

3.2.9 Na jednym serwerze Systemu kopii zapasowych (na jednej instancji systemu operacyjnego) mogą być zainstalowane minimum dwie bazy deduplikacyjne pozwalające zwiększyć skalowalność systemu.

3.3 Bezpieczeństwo

3.3.1 System kopii zapasowych musi zapewniać dostęp zintegrowany z usługą katalogową Active Directory, tj. „single sign on” – pojedyncze logowanie: użytkownik po zalogowaniu do domeny AD nie potrzebuje wykonywać następnego logowania, aby zarządzać Systemem kopii zapasowych poprzez konsolę administracyjną.

3.3.2 System kopii zapasowych musi zapewniać elastyczne delegowanie uprawnień oraz audytowanie działań użytkowników. Delegowanie uprawnień musi pozwalać na przydział uprawnień per serwer czy grupa serwerów, przydział uprawnień musi pozwalać na definiowanie uprawnień dla grup użytkowników z domeny AD.

3.3.3 System kopii zapasowych musi pozwalać na zarządzanie poprzez linię poleceń z tym, że uruchomienie jakiejkolwiek komendy/polecenia musi zostać poprzedzone koniecznością zalogowania (autentyfikacji) do systemu, funkcjonalność musi dotyczyć co najmniej platformy Windows i Linux,.

3.3.4 Komunikacja pomiędzy agentem a serwerem systemu musi opierać się na połączeniu szyfrowanym SSL.

3.3.5 System kopii zapasowych musi posiadać funkcjonalność blokowania danych do odczytu dla administratora -administrator systemu nawet mając pełne uprawnienia nie może odtworzyć danych, jeśli nie jest ich właścicielem, funkcjonalność ta musi być dostępna nie tylko dla danych z laptopów/desktopów, ale i dla serwerów (także dla danych plikowych i bazodanowych).

3.3.6 System kopii zapasowych musi pozwalać na skonfigurowanie mechanizmu podwójnej autentyfikacji administratora – do uruchomienia konsoli administracyjnej systemu potrzebne jest nie tylko logowanie, ale i dodatkowy tymczasowy kod wysyłany do administratora np. poprzez e-mail.

3.3.7 Szyfrowanie danych musi pozwalać na wybór algorytmu (minimum AES) także dla danych deduplikowanych na kliencie Systemu kopii zapasowych.

3.3.8 Możliwość szyfrowania musi pozwalać na elastyczny wybór miejsca szyfrowania: szyfrowanie danych na kliencie, szyfrowanie danych na serwerze backupowym i szyfrowanie tylko transmisji pomiędzy klientem backupowym a serwerem.

3.3.9 System kopii zapasowych musi wspierać mechanizm szyfrowania danych na napędach taśmowych LTO.

3.3.10 System kopii zapasowych musi pozwalać na ustawianie haseł dostępu do nośników tzw.: media password.

3.4 Raporty i alerty

3.4.1 System kopii zapasowych musi posiadać rozbudowany system powiadamiania o zdarzeniach poprzez e-mail.

3.4.2 System kopii zapasowych musi posiadać rozbudowany mechanizm raportowania dla administratorów, minimalny zestaw dostępnych raportów to:

- raport obciążenia/wykorzystania środowiska systemu,
- raport wykorzystania licencji (jeśli są limitowane),
- raport wykonanych zadań backupowych.

3.4.3 System kopii zapasowych musi mieć możliwość automatycznego wysyłania dowolnych raportów do wybranych użytkowników poprzez e-mail.

3.4.4 System kopii zapasowych musi mieć możliwość automatycznego zapisywania raportów w formacie PDF i HTML.

3.4.5 System kopii zapasowych musi pozwalać na definiowanie alertów per zadanie backupowe lub zadanie odtwarzania danych.

3.4.6 Notyfikacje alertów muszą być wysyłane co najmniej poprzez e-mail.

3.5 Funkcjonalność

3.5.1 System kopii zapasowych musi zapewniać funkcjonalność wznawiania zadań backupowych.

3.5.2 System kopii zapasowych musi zapewniać funkcjonalność równoległego wykonywania kopii danych backupowanych – inline copy (tego samego zestawu danych pojedynczego klienta) na minimum dwa docelowe urządzenia przechowywania danych.

3.5.3 System kopii zapasowych musi zapewniać funkcjonalność wykonywania zadania backupu wieloma równoległymi strumieniami – tzw. Multistreaming (agent systemu równolegle czyta różne obszary danych i bez pośredniczenia dysków automatycznie wysyła je do serwera, który zapisuje te dane albo na dyski albo na nośniki taśmowe). Funkcjonalność ta musi być dostępna dla dowolnych typów danych: backup plikowy, bazodanowy.

3.5.4 Funkcjonalność multistreamingu musi być dostępna dla deduplikacji bez względu na to, czy następuje na kliencie czy na serwerze systemu.

3.5.5 System kopii zapasowych musi zapewniać funkcjonalność multipleksowania kilku strumieni danych na nośniku taśmowym – tzw. multiplexing. Wydajny zapis wielu strumieni danych na taśmy bez pośrednictwa dysków.

3.5.6 System kopii zapasowych musi posiadać możliwość wykonywania backupu pełnego, przyrostowego, różnicowego oraz syntetycznego.

3.5.7 System kopii zapasowych musi oferować funkcjonalność backupu blokowego, polegającego na tym, iż agent buduje własną bazę zmian bloków danych, przez co backup przyrostowy nie wymaga odczytu całych plików tylko zmienionych bloków wielokrotnie przyspieszając backup. Funkcjonalność ta musi być dostępna minimum dla backupu danych plikowych.

3.5.8 System kopii zapasowych musi posiadać funkcję szyfrowania i kompresji danych transmitowanych przez LAN, możliwość wykorzystania szyfrowania i kompresji musi być dostępna w dowolnej kombinacji.

3.5.9 System kopii zapasowych ma realizować procesy backupu oraz odzyskiwania danych.

3.5.10 System kopii zapasowych ma umożliwić tworzenie zadań backupowych w oparciu o kalendarz.

3.5.11 System kopii zapasowych musi posiadać zintegrowane mechanizmy indeksowania pełnokontekstowego i wyszukiwania danych. System powinien mieć możliwość Indeksowania danych backupowanych i archiwizowanych. Licencja na indeksowanie pełnokontekstowe nie jest wymagana w tym postępowaniu.

3.5.12 System kopii zapasowych musi realizować funkcjonalność weryfikacji wykonanych kopii.

3.5.13 System kopii zapasowych umożliwia wykorzystanie funkcjonalności Bare Metal Restore dla odtwarzania systemu po awarii, wsparcie musi być dostępne minimum dla systemów Windows od wersji Windows Serwer 2012 R2 oraz Linux.

3.5.14 System kopii zapasowych musi posiadać funkcjonalność integracji z mechanizmami kopii migawkowych producentów pamięci masowych w szczególności : Dell, HP, NetApp, EMC, IBM, z tym, że takowy backup sterowany przez system a wykonywany przez daną macierz dyskową musi być dostępny nie tylko dla zasobów plikowych, ale również aplikacji: VMware, Hyper-V, MS SQL, MySQL. Zarządzanie kopiami migawkowymi musi odbywać się z konsoli administracyjnej systemu backupowego

3.5.15 System kopii zapasowych musi posiadać możliwość wykonywania kopii na urządzenia dyskowe i taśmowe.

3.5.16 System kopii zapasowych musi umożliwiać odtwarzanie danych plikowych pomiędzy systemami operacyjnymi np. odtwarzanie danych plikowych Linux na systemie Windows.

3.5.17 System kopii zapasowych musi pozwalać na odtwarzanie tylko samych uprawnień do plików.

3.5.18 System kopii zapasowych musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL).

3.5.19 System kopii zapasowych musi posiadać możliwość archiwizacji danych plikowych. Archiwizacja musi być realizowana jako jedno zadanie z kopią zapasową. W miejscu zarchiwizowanego pliku musi pozostać znacznik (link), do którego może odwołać się użytkownik końcowy.

3.5.20 System kopii zapasowych musi posiadać możliwość rozbudowy o funkcjonalność indeksowania i przeszukiwania zawartości plików leżących na backupie lub archiwum. Przeszukiwanie musi być realizowane za pomocą dedykowanej wyszukiwarki, w której wprowadzane będą szukane frazy i dostępne ono będzie dla użytkowników końcowych.

3.6 Środowisko fizyczne

3.6.1 System kopii zapasowych musi posiadać mechanizm tworzenia kopii otwartych plików na platformie Windows i Linux.

3.6.2 System kopii zapasowych musi wspierać wykonanie kopii na systemach klasy Linux i Unix.

3.6.3 System kopii zapasowych musi posiadać wsparcie co najmniej dla środowisk Linux, używanych przez Zamawiającego : RHEL, SuSe, Debian, Fedora, Gentoo, Ubuntu, Slackware

3.6.4 System kopii zapasowych musi posiadać szerokie wsparcie dla środowisk Unix, minimum: AIX, FreeBSD

3.6.5 System kopii zapasowych musi wspierać funkcjonalność odtwarzania fizycznego serwera do środowiska wirtualnego, minimum: dla serwera Windows do środowiska VMware.

3.6.6 System kopii zapasowych musi umożliwiać uruchamianie skryptów przed i po backupie, z tym, że musi posiadać mechanizm definiowania konta użytkownika, na którym te skrypty byłyby uruchamiane. Mechanizm ten musi być centralnie zarządzany poprzez konsolę administracyjną. Niedopuszczalna jest konieczność np. zmiany konta serwisowego dla danego agenta – konta serwisowe muszą być centralnie definiowane i zarządzane.

3.7 Środowisko wirtualne

3.7.1 System kopii zapasowych musi wspierać rozwiązania wirtualizacyjne: VMware, Hyper-V. To znaczy musi posiadać dedykowanego agenta do backupu minimum całej maszyny wirtualnej bez konieczności instalowania agenta wewnątrz maszyny.

3.7.2 System kopii zapasowych musi wspierać najnowsze wersje środowisk VMware poprzez integrację z vStorage API – backup i odtwarzanie danych musi być możliwe nie tylko poprzez sieć LAN, ale i SAN.

3.7.3 System kopii zapasowych musi integrować się z vCloud

3.7.4 System kopii zapasowych musi wspierać środowisko Hyper-V co najmniej dla :
- Microsoft Windows Server 2012,
- Microsoft Hyper-V Server 2012,
- Microsoft Windows Server 2012 R2,
- Microsoft Hyper-V Server 2012 R2,
- Microsoft Hyper-V Server 2016,
- Microsoft Hyper-V Server 2019.

3.7.5 System kopii zapasowych w kontekście platform VMware w przypadku kopii pliku VMDK musi wspierać granularne odtwarzanie pojedynczych plików.

3.7.6 System kopii zapasowych musi zapewniać automatyczne wykrywanie i dodawanie do polityki backupu nowych maszyn wirtualnych.

3.7.7 System kopii zapasowych musi umożliwiać odzyskanie i uruchomienie maszyn wirtualnych z kopii zapasowej bez oczekiwania na pełne przywrócenie maszyny wirtualnej – minimum dla VMware.

3.7.8 System kopii zapasowych musi umożliwiać odtworzenie z backupowanej maszyny wirtualnej VMware na środowisko Hyper-V.

3.7.9 System kopii zapasowych musi umożliwiać rozbudowę o moduł do zarządzania cyklem życia maszyn wirtualnych (włącznie z możliwością archiwizacji maszyn) co najmniej dla VMware.

3.7.10 System kopii zapasowych musi skalować się umożliwiając łatwą rozbudowę w miarę rozrastania się infrastruktury informatycznej. Rozbudowa nie może zakłócać bieżącej pracy systemu tworzenia kopii bezpieczeństwa.

3.7.11 System kopii zapasowych musi wspierać mechanizm CBT (change block tracking) minimum dla VMware i Hyper-V.

3.8 Aplikacje i bazy danych

3.8.1 System kopii zapasowych musi umożliwiać wykonanie kopii na gorąco bazy danych MySQL, PostgreSQL, na dowolnej platformie systemu operacyjnego (Windows/Linux/Unix) poprzez dedykowanego agenta bazodanowego, transfer danych musi odbywać się bez pośredniczenia dysków, a więc transfer danych z agenta bazodanowego bezpośrednio do serwera backupowego celem zapisu na dany nośnik.

3.8.2 System kopii zapasowych musi umożliwiać wykonanie kopii na gorąco bazy danych MS SQL na platformie Windows, konfiguracja agenta nie może powodować konieczności tworzenia skryptów uruchamianych po stronie klienta niezależnie od tego czy jest to serwer fizyczny czy wirtualny.

3.8.3 Odtwarzanie danych z backupu bazodanowego (MS SQL, MySQL) musi odbywać się poprzez konsolę administracyjną bez konieczności konfigurowania skryptów.

3.8.4 Konfiguracja agentów backupowych dla: MS SQL, MySQL musi odbywać się poprzez interfejs graficzny.

3.8.5 System kopii zapasowych musi umożliwiać wykonanie kopii na gorąco Active Directory za pomocą dedykowanego agenta, a następnie odzyskania pojedynczych obiektów oraz pojedynczych atrybutów AD wraz z hasłami użytkowników.

3.8.6 System kopii zapasowych musi umożliwiać odtwarzanie backupu wykonywanego online dedykowanym agentem, do pliku celem późniejszego odtwarzania bez udziały systemu. Funkcjonalność ta musi być dostępna minimum dla MS SQL.

3.8.7 System kopii zapasowych musi umożliwiać odtwarzanie pojedynczych tabel dla minimum: PostgreSQL, MySQL.

3.8.8 Dla minimum MySQL i PostgreSQL musi istnieć mechanizm backupu z wykorzystaniem mechanizmu backupu blokowego

3.8.9 Dla MS SQL możliwość skonfigurowania rozszerzenia pozwalającego backupować i odtwarzać bazy bezpośrednio z konsoli Management Studio

3.9 Archiwizacja

3.9.1 Zamawiający rozumie archiwizację danych, jako proces przenoszenia zasobów plikowych lub pocztowych do archiwum (repozytorium dyskowe lub taśmowe) z pozostawieniem skrótów lub bez ich pozostawiania.

3.9.2 Rozwiązanie Systemu kopii zapasowych musi pozwalać na archiwizację danych z możliwością pozostawiania znaczników na zasobach produkcyjnych (dla zasobów plikowych Windows\Linux\Unix i poczty Exchange), archiwizacja korzystać z tego samego repozytorium danych

3.9.3 System kopii zapasowych musi wspierać archiwizację zgodnych z wyznaczonymi kryteriami danych z systemów produkcyjnych na inne tańsze pamięci masowe. Mechanizm ten pozwoli na zmniejszenie ilości danych na systemach produkcyjnych

3.9.4 System kopii zapasowych musi obsługiwać strategię wielowarstwowego aktywnego archiwum (np. musi umożliwiać przenoszenie zarchiwizowanych plików lub wiadomości pomiędzy różnorodnymi urządzeniami pamięci masowej, w sposób zautomatyzowany przez politykę do wykonania krótko-, średnio- i długoterminowe okresów retencji, przy zachowaniu jedno krokowego odzyskiwania dla użytkowników końcowych

3.9.5 Moduł archiwizacji musi być zintegrowany z modułem do tworzenie kopii zapasowych w celu redukcji czasu okien backupowych przy zabezpieczaniu dużej ilości danych

3.9.6 System kopii zapasowych musi wspierać proces archiwizacji bezpośrednio na taśmy

3.9.7 System kopii zapasowych musi umożliwiać deduplikację danych archiwizowanych na poziomie bloków w celu redukcji ilości przestrzeni na dyskach fizycznych. Oprogramowanie musi umożliwiać globalną deduplikację dla archiwizacji i kopii zapasowych w celu minimalizowania zużycia pamięci masowej

3.9.8 Deduplikacja danych archiwizowanych Systemu kopii zapasowych musi odbywać się online blokowo a blok (segment) nie może być większy niż 128 KB

3.9.9 System kopii zapasowych musi zapewniać przezroczysty dostęp użytkowników do danych archiwalnych poprzez mechanizm skrótów

3.9.10 System kopii zapasowych musi umożliwiać administratorowi definiowanie wielu grup użytkowników z określonymi uprawnieniami wyszukiwania dla różnych poziomów dostępów (administrator, użytkownik zaawansowany, użytkownik).

3.9.11 System kopii zapasowych musi zapewnić opcję umożliwiającą weryfikację danych w celu zapewnienia, że dane są archiwizowane w sposób spójny i jest możliwe ich odzyskanie

3.9.12 Funkcjonalność odczytywania danych połączona ze zamianą danych na skróty musi pozwalać na tworzenie pełnej kopii danych poprzez mechanizm nazywany „incremental forever” lub „synthetic full”.

3.9.13 Oprogramowanie Systemu kopii zapasowych musi umożliwiać raportowanie wszystkich zadań archiwizacyjnych i odtworzeniowych dla celów zgodności z przepisami/normami bezpieczeństwa (compliance). System musi posiadać możliwość rozbudowy o funkcjonalność pełnokontekstowego indeksowania treści danych dla wybranych typów plików i wiadomości pocztowych (wraz z załącznikami), indeksacja musi odbywać się dla danych znajdujących się już w systemie. Licencja na pełnokontekstowe indeksowanie nie jest wymagana w tym postepowaniu.

3.9.14 Rozwiązanie Systemu kopii zapasowych musi pozwalać na archiwizację danych z możliwością pozostawiania znaczników na zasobach produkcyjnych (dla zasobów plikowych Windows\Linux\Unix.

3.9.15 System kopii zapasowych musi pozwalać archiwizować (z funkcjonalnością tworzenia skrótów) zasoby plikowe z systemów NAS.

3.9.16 Proponowane rozwiązanie Systemu kopii zapasowych musi umożliwiać zamianę plików na znaczniki (skróty) lub usuwanie plików po zarchiwizowaniu

3.10 Licencjonowanie

3.10.1 Oferowana licencja oraz architektura Systemu kopii zapasowych musi pozwalać na backup danych na nielimitowaną ilość bibliotek taśmowych i napędów fizycznych.

3.10.2 System kopii zapasowych musi zapewnić licencje minimum na:

- backup środowiska wirtualnego – 160 wirtualnych maszyn w środowisku VMware ESX wraz z aplikacjami,
- 1 agent dla backupu serwera Sharepoint zlokalizowanego w usłudze MS365
- Backup 100 skrzynek mailowych Exchange w usłudze MS365 z możliwością granularnego odtworzenia

3.10.3 Do dostarczonych licencji jest wymagane 36 miesięczne wparcie producenta (pierwsza i druga linia wsparcia świadczona w języku polskim) zapewniające wsparcie techniczne w trybie dni roboczych oraz dostęp do bezpłatnych ewentualnych poprawek i uaktualnień. Oferowane wsparcie serwisowe musi być świadczone przez producenta rozwiązania lub autoryzowanego partnera serwisowego producenta na terenie Polski. W przypadku serwisu świadczonego przez autoryzowanego partnera serwisowego producenta na terenie Polski wymagane jest potwierdzenie jakości świadczonych usług poprzez certyfikat ISO 9001:2015 lub ISO 9001:2008 na świadczone usługi serwisowe

3.10.4 Licencje Sytemu kopii zapasowych muszą być udzielone na czas nieoznaczony

4 Wdrożenie

4.1 Wdrożenie systemu

Wykonawca w porozumieniu z Zamawiającym musi przygotować plan wdrożenia i przedstawić go do akceptacji Zamawiającemu w ciągu 10 dni od podpisania umowy. Wykonawca przeprowadzi wdrożenie systemu kopii zapasowych w siedzibie Zamawiającego, w uzgodnionych godzinach dni roboczych, ustalonych z dwudniowym wyprzedzeniem, w taki sposób, aby nie wpływało ono na dostępność działających usług Zamawiającego. Wdrożenie będzie składało się z następujących etapów:

- Opracowanie szczegółowego harmonogramu wdrożenia
- Opracowanie polityk backupu
- Instalacja i konfiguracja systemu
- Testy akceptacyjne

4.1.1 Opracowanie polityk backupu

Zamawiający wymaga opracowania Polityk backupu dla poszczególnych serwerów. Każda polityka będzie zawierała między innymi takie informacje jak:

- Data i czas rozpoczęcia wykonywania kopii,
- Rodzaj kopii zapasowej,
- Gdzie kopia ma być przechowywana,
- Jak długo kopia ma być przechowywana,
- Jakie jest RTO dla danej polityki backupu.

4.1.2 Instalacja i konfiguracja systemu

Zamawiający wymaga opracowanie szczegółowego harmonogramu wdrożenia.
Wdrożenie musi składać się z co najmniej następujących czynności

- Instalacja systemu operacyjnego na serwerze fizycznym (zostanie dostarczony przez Zamawiającego) oraz oprogramowania do wykonywania kopii zapasowych,
- Konfiguracja repozytoriów na dane (dostarczone przez Zamawiającego i w ramach zamówienia)
- Ustawienie polityk do Backupu środowiska wirtualnego,
- Ustawienie polityk Backupu aplikacji i baz danych,
- Instalacja dedykowanych agentów,
- Konfiguracja modułu raportowania według wymagań Zamawiającego.
- Uruchomienia i konfiguracji wykonywania kopii zapasowej dla wskazanych skrzynek pocztowych Exchange w usłudze Microsoft 365.

4.1.3 Testy akceptacyjne

- Wykonanie w porozumieniu z Zamawiającym planu testów akceptacyjnych i przedstawienie do akceptacji Zamawiającemu – backup maszyny, odtworzenie, backup agentowy, odtworzenie granularne plików i baz danych.
- Wykonanie testów akceptacyjnych.

5 Gwarancja i wsparcie

Do dostarczonych licencji jest wymagane minimum 36 miesięczne wparcie producenta (pierwsza i druga linia wsparcia świadczona w języku polskim) zapewniające wsparcie techniczne w trybie dni roboczych oraz dostęp do bezpłatnych ewentualnych poprawek i uaktualnień. Oferowane wsparcie serwisowe musi być świadczone przez producenta rozwiązania lub autoryzowanego partnera serwisowego producenta na terenie Polski. W przypadku serwisu świadczonego przez autoryzowanego partnera serwisowego producenta na terenie Polski wymagane jest potwierdzenie jakości świadczonych usług poprzez certyfikat ISO 9001:2015 lub ISO 9001:2008 na świadczone usługi serwisowe.

6 Dokumentacja

Wykonawca wymaga dostarczenia dokumentacji technicznej powykonawczej wdrażanego rozwiązania. W szczególności dokumentacja powinna zawierać dane konfiguracyjne podczas instalacji i konfiguracji modułów systemu oraz uzgodnione polityki backupu, retencji i archiwizacji.

7 Szkolenie

Zamawiający wymaga przeprowadzenia 1 szkolenia z wdrażanego rozwiązania - min 8 godz. dla jednej grupy administratorów - 5 osób.