ZP.271.26.2024

Załącznik nr 9

Opis przedmiotu zamówienia.

Zadanie obejmuje:

1. **dostawę i wdrożenie dedykowanej macierzy do backupu wraz z oprogramowaniem w siedzibie Urzędu Gminy w Kaliskach (Nowowiejska 2, 83-260 Kaliska)**
2. **wykonanie odmiejscowienia backupu Urzędu Gminy w Kaliskach i wyniesienie do lokalizacji budynek Ochotniczej Straży Pożarnej w Kaliskach (ul. Nowowiejska 2b)**
3. **usługi przedwdrożeniowe i wdrożenie,**

i traktowane jest jako całość.

1. **Zamawiający wymaga dostarczenia i wdrożenia macierzy do backupu z dedykowanym oprogramowaniem oraz infrastrukturą sieciową, niezbędną do wykonania odmiejscowienia backupu na urządzeniu klasy NAS będącego własnością Zamawiającego (QNAP TS-431x).**

a) Wymagania minimalne dla macierzy do backupu z dedykowanym oprogramowaniem (dostawa i wdrożenie obejmują 1 komplet):

1. Zarządzanie i magazyny

1. Sprzęt musi być fabrycznie nowy, rok produkcji nie starszy niż 2024r.
2. System powinien być dostarczony w ramach sprzętowego appliance z zainstalowanymi i skonfigurowanymi wszystkim usługami, niezbędnymi do pracy systemu.
3. Rozwiązanie musi spełniać minimalne poniższe wymagania sprzętowe:
   a. Obudowa Rack 1U,
   b. Procesor: min. 6 rdzeni, min. 12 wątków. Minimalna częstotliwość bazowa procesora 2.9GHz,
   c. Pamięć RAM: min. 16GB DDR4,
   d. Przestrzeń dostępna na przechowywanie danych: min. 24 TB po RAID 5,
   e. Osobne dyski SSD M.2 NVME działające w RAID1 w celu instalacji warstwy oprogramowania i systemu operacyjnego,
   f. Redundantne zasilanie,
   g. Interfejsy sieciowe: min. 2 szt. Ethernet 1Gb,
   h. Gwarancja NBD on-premise o czasie trwania analogicznym do trwania wsparcia technicznego dla oprogramowania.
4. Produkt dostępny w polskiej wersji językowej.
5. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej.
6. System musi umożliwiać tworzenie kopii zapasowych na poziomie dysków.
7. System musi umożliwiać tworzenie kopii zapasowych na poziomie plików i folderów.
8. System musi umożliwiać replikację kopii zapasowych do wielu lokalizacji docelowych.
9. System musi umożliwiać tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT.
10. System musi umożliwiać współpracę z usługą kopiowania woluminów w tle (VSS) firmy Microsoft.

11. Możliwość zdefiniowania limitu przepustowości sieciowej z jakiej ma korzystać oprogramowanie backupowe.
12. System zarządzania nie może być oparty o relacyjne bazy danych.
13. Rozwiązanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej).
14. Rozwiązanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera (urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera (urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).
15. Aplikacje klienckie powinny wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn – serwer backupu/usługa zarządzania ani żaden inny element Systemu, nie powinien brać udziału w przesyłaniu danych.
16. Rozwiązanie musi być systemem multi-storage i umożliwia tworzenie wielu repozytoriów danych jednocześnie również na innych środowiskach jako przestrzeń do replikacji danych.
17. System musi oferować mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.
18. System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami.
19. System musi umożliwiać wykonywanie kopii obrazu dysku, kopii plików i katalogów oraz kopii maszyn wirtualnych bez ich zatrzymywania z zachowaniem stuprocentowej integralności i spójności danych wewnątrz wykonanej kopii zapasowej.
20. Rozwiązanie musi realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie.
21. Rozwiązanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.
22. System musi umożliwiać automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku wystąpienia błędu.
23. Rozwiązanie powinno umożliwiać klonowanie planów kopii zapasowych, planów replikacji oraz planów testowego odtwarzania maszyn wirtualnych.
24. Rozwiązanie powinno umożliwiać uruchamianie przy zadaniach backupu dowolnych skryptów PRE/POST oraz po wykonaniu migawki VSS.
25. System powinien umożliwiać definiowanie tzw. okna backupowego dla każdego z zadań w celu umożliwienia zarządzania obciążeniem sieci i uwzględnienia okien serwisowych występujących u Zamawiającego.
26. System musi automatycznie dodawać do polityki i harmonogramu tworzenia backupów nowe źródła / maszyny wirtualnych, dodane do bieżącego środowiska (automatyzacja oparta na polityce tworzenia kopii).
27. Rozwiązanie musi udostępniać możliwość podglądu postępu działania dowolnego zadania, w tym zadania wykonywania kopii zapasowych, odtwarzania danych, testowego odtwarzania danych, usuwania danych oraz zadania odświeżania zajętości magazynu na dane.
28. Rozwiązanie musi posiadać system powiadamiania poprzez e-mail oraz Slack o zdarzeniach w następujących przypadkach: zadanie zostało zakończone pomyślnie, zadanie zostało zakończone z ostrzeżeniami, zadanie zostało zakończone z błędem, zadanie zostało anulowane, zadanie nie zostało uruchomione.
29. System powinien umożliwiać wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika.
30. Oferowane rozwiązanie musi być dobrane pod względem wydajności w oparciu o najlepsze praktyki producenta.
31. Rozwiązanie musi być wyskalowane, dobrane pod względem wymaganej funkcjonalności i wydajności stosownie do ilości zabezpieczanych danych i obiektów z uwzględnieniem przyrostu danych (serwery, maszyny wirtualne, bazy danych itp.) zgodnie z opisem w zapytaniu ofertowym.

32. Wydajność oferowanej konfiguracji musi być taka, aby wszystkie funkcje systemu były dostępne w chwili wdrożenia (np. deduplikacja, kompresja, instancja workerów i browserów, replikacja, testowe odtwarzanie maszyn wirtualnych).
33. System pozwala na zmniejszenie rozmiaru przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych.
34. Proces deduplikacji musi być możliwy dla każdego z typów obsługiwanych magazynów.
35. Proces deduplikacji nie może wymagać instalacji żadnych dodatkowych komponentów, które będą pośredniczyły w zapisie danych z deduplikowanych.
36. Proces deduplikacji nie może posiadać pojedynczego punktu awarii, tym samym musi być dostępny jednocześnie na każdym wspieranym magazynie na dane - również replikacyjnych. Awaria jednego z magazynów na dane nie może wpłynąć na integralność deduplikatów, jak i tablicy deduplikatów na innym magazynie.
37. Proces deduplikacji realizowany jest blokiem o stałej wielkości, którego wielkość może zostać ustalona na etapie wdrożenia rozwiązania zgodnie z najlepszymi praktykami producenta.
38. Proces szyfrowania kopii zapasowych nie może ograniczać procesu deduplikacji w ramach tego samego klucza szyfrującego.
39. Kompresja kopii zapasowych musi obsługiwać jeden z wymienionych algorytmów: LZ4, ZStandard. Dodatkowo, musi umożliwiać określenie szczegółowego poziomu kompresji, w tym: niski, średni, wysoki.
40. Instalacja, modyfikacja ustawień, polityki tworzenia kopii zapasowej systemu nie może wymagać przerwania pracy lub restartu systemu.
41. System musi pozwalać na automatyczne aktualizacje oprogramowania.
42. System musi być w stanie kompresować i szyfrować zabezpieczone dane w systemach NAS.
43. System musi pozwalać na uruchomienie kontenerów Docker w dowolnych urządzeniach NAS i innych środowiskach w celu ich zabezpieczenia.
44. System tworzenia kopii zapasowej musi przechowywać dane w sposób zapewniający ich niezmienność (tzw. "resilience"), dzięki czemu kopie zapasowe nie będą mogły zostać nadpisane lub zmodyfikowane przez cały okres ich przechowywania, retencji.
45. System zarówno będzie przechowywać dane w kopii zapasowej w postaci zaszyfrowanej jak też ruch wewnątrz systemu również musi być szyfrowany.
46. Archiwum długoterminowych kopii zapasowych musi być szyfrowane, a odzyskiwanie z archiwum obsługiwane z tego samego interfejsu użytkownika, co inne przywracanie dane.
47. System musi mieć mechanizmy chroniące przejęcie konta administratora oraz umożliwiać definiowanie dodatkowych uprawnień dla każdej z predefiniowanych ról użytkowników.
48. System musi pozwalać na gradację uprawnień administratorów - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: system operator, backup operator, restore operator, viewer. Dla każdej z tych ról system musi umożliwiać przypisywanie dodatkowych uprawnień, w tym możliwość zablokowania usuwania danych.
49. Rozwiązanie musi posiadać możliwość nieodwracalnego usuwania danych z magazynu na dane w momencie spełnienia dodatkowych wymogów.
50. W sytuacji, gdyby podstawowe urządzenie tworzenia kopii zapasowej było niedostępne, system musi posiadać możliwość przywrócenia z archiwum za pomocą innej instancji systemu dostarczonej przez tego samego producenta. tzn. archiwum musi zawierać wszystkie informacje konieczne do odzyskania.
51. Rozwiązanie musi umożliwiać uruchomienie konsoli w chmurze producenta zlokalizowanej na terenie Polski, w celu umożliwienia dostępu do środowiska zarządzania kopiami zapasowymi w przypadku czasowej niedostępności środowiska lokalnego.
52. System kopii zapasowej musi umożliwiać dostęp do konsoli administracyjnej z wielu stacji roboczych.
53. System kopii zapasowej musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.

54. System powinien posiadać predefiniowane schemat tworzenia kopii zapasowych, min. Custom, Basic, G-F-S, Forever incremental.
55. Rozwiązanie musi obsługiwać kontrolę dostępu opartą na rolach (RBAC).
56. Możliwość składowania utworzonych kopii zapasowych na magazynach chmurowych Amazon AWS, Azure, Wasabi, Google Cloud Storage, Backblaze B2, magazyny zgodne z S3 oraz dedykowana chmura producenta appliance'u.
57. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych po protokole smb, S3, nfs, iscsi, katalog lokalny.
58. Zarządzanie i odzyskiwanie danych z kopii musi odbywać się z tego samego interfejsu użytkownika (konsoli), niezależnie od tego, gdzie znajduje się kopia zapasowa (w chmurze AWS, Azure, GCP, w Data Center czy w usłudze typu SaaS).
59. Czas przechowywania kopii zapasowej (retention time) systemu backupu nie może być zmieniony np. poprzez manipulowanie wskazaniami zegara serwera NTP w celu szybszego ich wyekspirowania - tzn. czasy przechowywania kopii zapasowych nie będą zależne od wskazań zegara czasu serwera NTP, ale będą wykorzystywać technologię, która mierzy upływ czasu.
60. Możliwość generowania raportów dobowych w oparciu o harmonogram.
61. Produkt musi posiadać możliwość zapisu kopii zapasowych do magazynu chmurowego dostarczanego bezpośrednio przez producenta oprogramowania (data center powinno być zlokalizowane na terenie Polski).
62. Produkt musi posiadać możliwość zdefiniowania maksymalnej liczby równocześnie backupowanych urządzeń w ramach jednego planu backupowego, niezależnie od typu urządzenia (np. stacja robocza, serwer, maszyna wirtualna).
63. Możliwość wyświetlenia szczegółowych informacji o chronionym urządzeniu takich jak: CPU, RAM, System operacyjny, Adres IP.
64. Produkt musi posiadać możliwość zdefiniowania poziomu obciążenia magazynu, po osiągnięciu którego zostanie wysłane powiadomienia e-mail (poziom definiowany indywidualnie dla każdego magazynu).

2. Wspierane systemy

Możliwość instalacji oraz uruchomienia agenta backupowego na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy:

- Alpine 3.10+,
- Debian: 9+,
- Ubuntu: 16.04+,
- Fedora: 29+,
- centOS: 7+,
- RHEL: 6+,
- openSUSE: 15+,
- SUSE Enterprise Linux (SLES): 12 SP2+,
- macOS: 10.13+,
- Windows: 7, 8.1, 10(1607+),
- Windows Server: 2008 R2+,

Środowisk wirtualnych:

- Hyper-V 2016+,
- VMware: 6.7+.

3. Środowiska fizyczne i bazy danych

1. Rozwiązanie powinno umożliwiać tworzenie grup urządzeń w celu automatyzacji procesów podczas pracy z urządzeniami.

2. Produkt musi posiadać możliwość tworzenia zadań dla grupy urządzeń oraz dla wybranych urządzeń.
3. Rozwiązanie musi pozwalać na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej.
4. Rozwiązanie backupowe musi pozwalać na zabezpieczanie zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption.
5. System jest niezależny od wersji Microsoft SQL i musi umożliwiać przywracanie danych SQL dla tej samej lub nowszej wersji.
6. System musi obsługiwać również narzędzia RMAN firmy Oracle do tworzenia kopii zapasowych i odzyskiwania. Dodatkowo system musi obsługiwać funkcję przyrostowego scalania danych.
7. System kopii zapasowej musi wspierać odtwarzanie pojedynczych plików z systemów Windows oraz Linux.
8. W przypadku niedostępności źródła danych, system musi oczekiwać na powrót dostępności źródła danych przez określony przez administratora okres. W przypadku braku powrotu dostępności źródła, system musi podjąć ustaloną przez administratora liczbę prób kontynuacji kopii. W przypadku powrotu źródła danych system musi kontynuować zadanie backupu od momentu, w którym wystąpiła niedostępność źródła - system nie może rozpoczynać zadania od punktu początkowego i rozpoczynać przesyłania kopii od zera. W przypadku braku powrotu źródła danych system powinien zakończyć zadanie błędem.
9. Odtwarzanie Bare Metal Restore w Systemie może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.
10. Rozwiązanie powinno umożliwiać uruchamianie procesu Bare Metal Restore z dowolnego boot-owalnego nośnika danych.
11. Rozwiązanie powinno wspierać odtwarzanie danych w scenariuszach P2P, P2V, V2P, V2V.
12. Rozwiązanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie (RAW, VHD, VHDX, VMDK).
13. Rozwiązanie musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL) oraz z prawami dostępu. Funkcjonalność ta musi być możliwa do skonfigurowania przez administratora na etapie konfiguracji procesu przywracania danych.
14. Rozwiązanie musi umożliwiać przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows).

4. Środowiska wirtualne

1. System musi wspierać kopię w trybie application-aware dla wszystkich wspieranych wirtualizatorów.
2. System musi umożliwiać wykonywanie kopii maszyn wirtualnych z zastosowanie zaawansowanych metod transportu (HotAdd, SAN, LAN), w tym metodami LAN-Free, tj. takimi, które podczas wykonywania backupu nie obciążają interfejsów sieciowych maszyn wirtualnych.
3. System kopii zapasowej musi wykorzystywać mechanizmy Change Block Tracking oraz Replica Change Tracking dla wspieranych przez producenta platformach wirtualizacyjnych.
4. Rozwiązanie producenta musi być certyfikowane przez dostawcę platformy wirtualizacyjnej, tj. producent musi uczestniczyć w programie Technology Alliance Partner.
5. System kopii zapasowej musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage-u użytego do przechowywania kopii zapasowych.

6. Dla środowiska vSphere i Hyper-V rozwiązanie powinno umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).
7. System kopii zapasowej musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere.
8. System kopii zapasowej musi umożliwiać weryfikację odtwarzalności wirtualnych maszyn według własnego harmonogramu w dowolnym środowisku.

5. Aplikacje SaaS

1. Ochrona z tej samej konsoli dla Microsoft 365 min. na poziomie, skrzynek pocztowych, onedrive, kontaktów, kalendarza.
2. Rozwiązanie musi umożliwiać przywracanie danych Microsoft 365: do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku .pst oraz do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji).
3. System musi umożliwiać granularne odtwarzanie danych, tj. pojedynczych plików z kopii obrazu dysku oraz pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365.
4. System musi umożliwiać zabezpieczanie środowisk Git, w tym GitHub, GitLab oraz Bitbucket wraz z metadanymi.
5. System musi umożliwiać odtworzenie dowolnego środowiska Git w dowolnym innym środowisku Git, tzw. odtwarzanie crossowe.
6. System musi umożliwiać zabezpieczenie metadanych zebranych wokół repozytorium w ramach zabezpieczanego środowiska Git.
7. System musi umożliwiać odtwarzanie metadanych repozytorium Git do dowolnego innego środowiska Git w przypadku chęci odtworzenia repozytorium.
8. System musi umożliwiać zabezpieczenie środowisk Jira.
9. System musi umożliwiać odtworzenie środowiska Jira do chmury lub środowiska lokalnego.

6. Licencjonowanie i wsparcie techniczne

1. Wszystkie linie support-u muszą być obsługiwane w języku polskim.
2. Wsparcie techniczne musi być świadczone bezpośrednio przez główną siedzibę producenta.
3. Możliwość zgłaszania ticketów supportowych bezpośrednio z poziomu interfejsu zarządzania w formie czatu.
4. Producent wraz z rozwiązaniem musi udostępnić materiały samopomocowe w j. polskim (minimum dostęp do bazy wiedzy, materiałów wideo oraz kart produktów).
5. Wsparcie techniczne musi umożliwiać korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego.
6. W ramach wsparcia technicznego Zamawiający musi mieć dostęp do tzw. Dedicated Customer Success Managera, tj. osoby po stronie Dostawcy dedykowanej do obsługi zgłoszeń technicznych, doraźnej pomocy i bieżącej pomocy w utrzymania infrastruktury Zamawiającego.
7. W ramach dokumentacji posprzedażowej Dostawca musi dostarczyć bezpośredni numer telefonu oraz adres e-mail do Dedicated Customer Success Managera.
8. Licencje w ramach rozwiązania powinny pozwalać na zabezpieczenie: nielimitowanej ilości maszyn wirtualnych, nielimitowanej ilości serwerów fizycznych, nielimitowanej ilości stacji roboczych.
9. Licencje powinny być dostępne w opcji wieczystej. Wsparcie techniczne nie powinno być wymagane dla poprawnego działania systemu.
10. Wsparcie techniczne producenta musi zostać dostarczone na min. 24 miesiące.
11. Licencje powinny umożliwiać replikacje na własne zasoby.
12. Licencje powinny umożliwiać skorzystanie z przestrzeni chmurowej dostarczonej bezpośrednio przed producenta, min. 4.8TB przez cały okres trwania gwarancji NBD na warstwę sprzętową. Zamawiający w dalszej eksploatacji systemu chciałby mieć możliwość skorzystania.

7. Anty-ransomware i bezpieczeństwo

1. System plików rozwiązania musi być odporny na ataki Ransomware (zapewnić ochronę przed szyfrowaniem end-to-end, kopie zapasowe nie mogą być nadpisywane - "niezmienny system plików").
2. System powinien umożliwiać wykorzystanie wbudowanego menedżera haseł do przechowywania wszelkich sekretów (haseł, danych dostępowych, kluczy szyfrujących) wykorzystywanych przez System.
3. System powinien umożliwiać przywrócenie hasła głównego administratora w przypadku jego utraty.
4. W ramach systemu, komunikacja pomiędzy hostem źródłowym, a magazynem powinna odbywać się tylko i wyłącznie bezpośrednio pomiędzy agentem backupu, a magazynem. Komunikacja nie może przechodzić przez serwer backupu ani żaden inny komponent, którego awaria sparaliżowałaby działanie Systemu. System nie może posiadać pojedynczego punktu awarii.
5. System musi działać w zgodzie z regułą Zero-knowledge Encryption. Oznacza to, że wszelkie sekrety muszą być przechowywane w centralnym Managerze Haseł w postaci zaszyfrowanej algorytmem AES i być udostępniane agentowi dopiero w momencie rozpoczęcia wykonywania kopii zapasowej. Sekrety nie mogą być przechowywane w konfiguracji agenta na zabezpieczanym urządzeniu.

2. Wykonanie odmiejscowienia backupu Urzędu Gminy w Kaliskach i wyniesienie go do budynku Ochotniczej Straży Pożarnej w Kaliskach (ul. Nowowiejska 2b).

Posiadane przez Zamawiającego urządzenie backupu QNAP TS-431x należy:
-wyposażyć w 4 dyski 8TB każdy, przeznaczone do pracy w urządzeniach klasy NAS i w pełni kompatybilne z posiadanym urządzeniem NAS,
-zainstalować urządzenia w szafie w budynku OSP w Kaliskach,
-połączyć z siecią LAN Zamawiającego, z wykorzystaniem dostarczanych również w ramach niniejszego zadania, urządzeń sieciowych o parametrach nie niższych niż opisane poniżej,
-wykonawca będzie zobowiązany dostarczyć wszelki pozostały sprzęt sieciowy, niewyspecyfikowany w zadaniu, a niezbędny do realizacji zadania,
-wdrożyć jako dodatkowe repozytorium zapasowe do urządzenia opisanego w punkcie A).

Realizowane, dedykowane połączenie do repozytorium zapasowego systemu kopii zapasowych, musi spełniać następujące wymagania:
- MTU min 1504 bajty,
- przepustowość min. 760 Mb/s oraz 1480 kpps dla pakietów o rozmiarze 64 bajtów,
- przepustowość min. 990 Mb/s oraz 340 kpps dla pakietów o rozmiarze 512 bajtów,
- MTBF min. 180 tys. godzin,
- akceleracja sprzętowa protokołu IPSec.

Powyższe urządzenia sieciowe należy dostarczyć wraz z kompletem okablowania, zasilaczy, adapterów i akcesoriów montażowych, zainstalować w lokalizacjach Zamawiającego, uruchomić i przetestować, zgodnie z powyższymi zapisami.
Jeżeli niezbędne będzie wybudowanie niezbędnego medium transmisyjnego, wykona to wykonawca.

Wykonawca musi również przewidzieć zabezpieczenie wymaganej przestrzeni montażowej, potrzebnej na zainstalowane powyższych urządzeń sieciowych.

ZP.271.26.2024

3. Usługi przedwdrożeniowe i wdrożenia.

W ramach usług wdrożenia Wykonawca wykona usługi polegające przede wszystkim na:

a) przygotowaniu koncepcji i harmonogramu wdrożenia systemu wraz odmiejscowieniem,

W ramach przygotowania koncepcji wdrożenia systemu Wykonawca zobowiązuje się do:
- przeprowadzenia analizy przedwdrożeniowej, której celem jest zrozumienie specyficznych potrzeb i wymagań Zamawiającego,
- przeprowadzenia szczegółowego przeglądu aktualnego systemu backupu, w tym m. in.:
  - przedmiotu i metody wykonywania backupu,
  - harmonogramu i autoryzacji backupów,
  - zabezpieczenia dostępu do kopii,
  - monitorowania procesu oraz aktualizacji procedur,
  - oraz wszelkich związanych z tym komponentów, programów i usług,
- oceny aktualnej skuteczności i zgodności z najlepszymi praktykami w zakresie zabezpieczenia i odkładania danych,
- do uwzględnienia wykonania prac wdrożeniowych wymagających całkowitego wyłączenia dostępu do sieci w dni wolne od pracy Urzędu po wcześniejszym uzgodnieniu z Zamawiającym.

Wykonawca przedstawi po uwzględnieniu wymagań Zamawiającego do akceptacji opis architektury wybranego rozwiązania, w tym projekt wdrożenia systemu backupu, który musi zawierać co najmniej: opis funkcjonalny systemu, wykaz wymaganych elementów systemu, sposób ich wdrożenia i konfiguracji, szczegółowy opis architektury proponowanego rozwiązania wraz z opisem integracji z infrastrukturą techniczną Zamawiającego wraz z planem wdrożenia obejmującym harmonogram działań.

b) wykonanie wdrożenia, przy aktywnym udziale personelu Zamawiającego, na podstawie zaakceptowanej przez Zamawiającego koncepcji i harmonogramu, w tym:

- dostawy, instalacji i uruchomienia oferowanego sprzętu,
- rozbudowy posiadanej przez Zamawiającego macierzy NAS o dostarczane dyski oraz jej konfiguracja,
- instalacja agentów oprogramowania do wykonywania kopii zapasowych na serwerach i urządzeniach końcowych Zamawiającego,
- wdrożenie polityk usprawniających podłączanie nowego sprzętu Zamawiającego do systemu kopii zapasowych,
- połączenie wszystkich urządzeń Zamawiającego przewidzianych na etapie analizy do wdrażanego systemu,
- instalacja odmiejscowionego repozytorium zapasowego oraz jego konfiguracja w ramach spójnego systemu,
- zaaplikowanie zaplanowanych polityk wykonywania kopii zapasowych.

c) przeprowadzenie testów po wdrożeniu w celu weryfikacji poprawności działania systemu oraz optymalizacja konfiguracji systemu na podstawie przeprowadzonych testów
d) przygotowanie dokumentacji powykonawczej:

Dokumentacja powykonawcza musi zawierać procedury administracyjne i operacyjne oraz inne informacje, istotne w eksploatacji systemu, w tym co najmniej:
- procedury i instrukcje dotyczące instalacji, konfiguracji i aktualizacji systemu,
- procedury dotyczące wykonywania i przechowywania kopii,
- instrukcje dla administratorów, w tym procedury zarządzania urządzeniami,

- inne niezbędne dokumenty, jakie powstaną w trakcie realizacji wdrożenia systemu, uzgodnione z przedstawicielami Zamawiającego.

Dokumentacja musi być przekazana w wersji elektronicznej i napisana w języku polskim. Procedury i instrukcje producenta mogą być przekazane w języku angielskim lub polskim.