

## Szczegółowy Opis Przedmiotu Zamówienia

w postępowaniu pn.: „Dostawa urządzenia do gromadzenia kopii bezpieczeństwa infrastruktury krytycznej Urzędu Miasta Szczecin”

1. Rozwiązanie musi być spójnym, dedykowanym urządzeniem przeznaczonym do przechowywania danych kopii zapasowych (appliance). Całość zaoferowanego rozwiązania musi pochodzić od tego samego producenta – nie dopuszcza się integrowania urządzeń i oprogramowania różnych producentów w celu realizacji poniższych wymagań.
2. Rozwiązanie musi być niezależne od używanego oprogramowania do wykonywania kopii zapasowych.
3. Rozwiązanie musi być obecne na rynku i dostępne w autoryzowanym kanale sprzedaży producenta od minimum trzech lat.
4. Rozwiązanie musi mieć możliwość instalacji w standardowej szafie rack 19". Wraz z urządzeniami składającymi się na rozwiązanie należy dostarczyć komplet kabli (zasilających, sieciowych, połączeniowych, itp.).
5. Rozwiązanie musi udostępniać zasoby do systemu kopii zapasowych z wykorzystaniem minimum protokołów CIFS i NFS.
6. Rozwiązanie musi umożliwiać skonfigurowanie minimum trzech różnych serwerów czasu (NTP), w tym co najmniej jednego w sieci LAN i jednego w Internecie, w celu zapobieżenia atakom typu „NTP Spoofing”.
7. Rozwiązanie musi umożliwiać optymalizację składowania długoterminowego poprzez efektywne mechanizmy kompresji i/lub deduplikacji danych. Realizacja tego wymagania może być wykonywana inline, adaptacyjnie bądź jako proces działający w tle, pod warunkiem spełnienia opisywanych wymagań pojemnościowych i wydajnościowych.
8. Rozwiązanie musi zapewniać globalną deduplikację, tj. przechowywać jedynie unikalne bloki danych, niezależnie od tego, jakim protokołem bądź do jakiego udziału zostały zapisane. Nie jest dopuszczalne tworzenie unikalnej bazy deduplikatów per protokół bądź per udział.
9. Rozwiązanie musi pozwalać na udostępnienie zasobów do różnych aplikacji do wykonywania kopii zapasowych jednocześnie. Jeżeli konkretne wymaganie nie stanowi inaczej (tj. nie wskazuje konkretnej funkcji używanej przez Zamawiającego aplikacji), poniższe wymagania muszą być realizowane dla dowolnej aplikacji do wykonywania kopii zapasowych.
10. Rozwiązanie musi być wyposażone w minimum 2 interfejsy 1 GbE ze złączem RJ-45 oraz minimum 2 interfejsy 25 GbE z wkładkami 25GBASE-SR.
11. Architektura rozwiązania musi uwzględniać wysoką dostępność i obejmować co najmniej:
  - a. dyski wymienne w trakcie pracy urządzenia,
  - b. redundantne zasilacze wymienne w trakcie pracy urządzenia,
  - c. wszystkie zainstalowane dyski w konfiguracji RAID-6 z zapasowym dyskiem "hot-spare",
  - d. redundantne wentylatory.
12. Pojemność rozwiązania musi umożliwiać wykonywanie kopii zapasowej 50TB danych źródłowych, których kopie zapasowe będą przechowywane z następującą retencją: kopie codzienne przez okres 14 dni, pełne kopie tygodniowe przez okres 8 tygodni, pełne kopie miesięczne przez okres 12 miesięcy oraz pełne kopie roczne przez okres 1 roku.

13. Dla wybranych zestawów chronionych danych, rozwiązanie musi umożliwiać wykonywanie zadań backupu pełnego i nie mniej niż 60 kopii przyrostowych do wykonania kolejnego backupu pełnego bądź syntetycznego.
14. Zakładany roczny przyrost ilości danych źródłowych to 2-5%.
15. Niezależnie od powyższego, minimalna dostarczana pojemność użytkowa dla pojedynczego urządzenia (po skonfigurowaniu odpowiedniej nadmiarowości) dysków nie może być niższa niż 150 TB.
16. Jeżeli dostarczona pojemność użytkowa nie będzie wystarczająca do przechowywania danych źródłowych z retencją opisaną w punkcie 12, Wykonawca będzie zobowiązany do dostarczenia rozbudowy pojemności na swój koszt w taki sposób, żeby umożliwić zrealizowanie zadanej retencji dla właściwych kopii zapasowych.
17. Rozwiązanie musi współpracować (być oficjalnie wspierane) z oprogramowaniem do ochrony danych Veeam Backup & Replication. Za rozwiązanie oficjalnie wspierane uważa się rozwiązanie opisane na stronie producenta pod adresem [https://helpcenter.veeam.com/docs/backup/vsphere/deduplicating\\_storage\\_appliances.html?ver=120](https://helpcenter.veeam.com/docs/backup/vsphere/deduplicating_storage_appliances.html?ver=120).
18. Dla zwiększenia wydajności i bezpieczeństwa, rozwiązanie musi umożliwiać wymianę danych z użytkowanym przez Zamawiającego oprogramowaniem Veeam Backup & Replication poprzez natywny dla tego oprogramowania komponent Veeam Accelerated Data Mover. Dopuszcza się realizację tego wymogu poprzez uruchomienie komponentu na systemie operacyjnym dostarczanego urządzenia bądź poprzez zapewnienie dedykowanego serwera zewnętrznego z uruchomioną usługą Veeam Data Mover Service, z uwzględnieniem punktu 0 niniejszych wymagań - tj. wyprodukowanego, dostarczonego i obsługiwanego przez tego samego producenta, co pozostałe urządzenia wchodzące w skład rozwiązania.
19. Rozwiązanie musi umożliwiać rozbudowę do pojemności użytecznej 800 TB bez konieczności wymiany żadnych istniejących komponentów z zachowaniem pojedynczej, spójnej bazy deduplikatów.
20. Producent musi gwarantować niezmiennosc ceny na rozbudowę rozwiązania o kolejne urządzenie wchodzące w skład oferowanej konfiguracji w cenie nie wyższej niż koszt pojedynczego urządzenia dostarczanego inicjalnie. Gwarancja taka musi obowiązywać minimum przez cały okres trwania wsparcia producenta, opisanego w punkcie 35.
21. Producent urządzeń wchodzących w skład rozwiązania musi pisemnie gwarantować, iż oferowane urządzenia nie zostaną objęte klauzulą zakończenia wsparcia (End-of-support) w okresie co najmniej 5 lat od podpisania przez Zamawiającego protokołu odbioru zamówienia. W przypadku objęcia w tym czasie dostarczonych urządzeń powyższą klauzulą, Oferent zobowiązany będzie do wymiany dostarczonych urządzeń na nowsze, nie objęte taką klauzulą wraz z przeprowadzeniem całkowitej migracji przechowywanych danych na własny koszt.
22. Całkowita przepustowość pojedynczego urządzenia podczas tworzenia kopii zapasowych musi wynosić nie mniej niż 15 TB/h. Przepustowość ta musi być potwierdzona dokumentacją producenta. Osiągnięcie wymaganej przepustowości nie może powodować obciążenia systemu chronionego, a jedynie być wewnętrzną przepustowością urządzenia - tj. nie może uwzględniać autorskich mechanizmów optymalizacji danych mających wpływ na wydajność systemu chronionego lub serwera backupu, takich jak EMC DDBoost, HPE Catalyst, DXi Accent lub podobnych.
23. Jeżeli jakkolwiek z opisywanych w niniejszym dokumencie funkcjonalności wymaga dostarczenia licencji na pojedyncze urządzenie, pojedynczy kontroler, półkę dyskową bądź licencji pojemnościowej, należy dostarczyć je na całkowitą dostarczaną pojemność rozwiązania.

24. Rozwiązanie musi oferować możliwość wykonywania replikacji do/z urządzenia tego samego producenta w drugim ośrodku przetwarzania danych. Transfer danych do drugiego ośrodka musi się odbywać się przez sieć WAN w taki sposób, aby minimalizować wykorzystanie przepustowości łącza (wysyłanie wyłącznie zmienionych bloków). Jeśli do replikacji wymagana jest licencja, należy dostarczyć ją na całkowitą dostarczaną pojemność rozwiązania dla urządzenia źródłowego i docelowego.
25. Rozwiązanie musi obsługiwać logowanie do interfejsu zarządzającego przy użyciu uwierzytelniania dwuskładnikowego (2FA), które polega na integracji poświadczeń użytkownika z generatorem jednorazowych haseł dostarczanych użytkownikowi pocztą elektroniczną, SMS bądź za pomocą aplikacji na smartfona.
26. Rozwiązanie musi umożliwiać przyznawanie użytkownikom ról o różnych poziomach uprawnień (Role-based Access Control), w tym co najmniej użytkownika (tylko prawa do przeglądania), operatora (prawa do nieniszczących zmian) i administratora (z najszerzym zakresem uprawnień).
27. Wymagane jest, aby role można było skonfigurować w taki sposób, aby żaden użytkownik, niezależnie od poziomu uprawnień, nie mógł samodzielnie zmienić lub wyłączyć ochrony przed skutkami oprogramowania ransomware, o którym mowa w sekcji 30, ani spowodować innych uszkodzeń danych, takich jak usunięcie udostępnionego zasobu wraz z jego zawartością.
28. Rozwiązanie musi umożliwiać szyfrowanie przechowywanych danych. Jeżeli włączenie szyfrowania danych spowoduje obniżenie wydajności urządzenia w stosunku do wymagań opisanych w sekcji 22, należy dostarczyć urządzenie odpowiednio bardziej wydajne tak, aby realizowało ono wymagania tej sekcji.
29. Rozwiązanie musi być w stanie wykryć i powiadomić administratora o potencjalnych niepożądanych działaniach w ramach udostępnionych udziałów, takich jak usunięcie znacznej ilości danych lub zaszyfrowanie danych.
30. Rozwiązanie musi posiadać zintegrowany mechanizm "antyransomware", umożliwiający odzyskanie danych zaszyfrowanych/uszkodzonych/usuniętych przez ransomware, błąd ludzki lub celowe działanie.
31. Mechanizm „antyransomware” musi być niezależny od używanego oprogramowania do tworzenia kopii zapasowych i musi być oparty jedynie o wewnętrzne mechanizmy dostarczanego rozwiązania.
32. Mechanizm "antyransomware" nie może negatywnie wpływać na działanie oprogramowania do tworzenia kopii zapasowych.
33. Mechanizm „antyransomware” musi zabezpieczać dane poprzez tworzenie minimum dwóch niezależnych kopii aktualnego łańcucha zadań backupowych w jednej lokalizacji. Jeśli pierwsza kopia zostanie uszkodzona, zaszyfrowana lub usunięta, dane muszą być w pełni odtwarzalne z drugiej kopii, jak opisano w sekcji 30. Jeśli do realizacji tego wymagania konieczne jest dostarczenie dodatkowych urządzeń, muszą one zostać dostarczone wraz z odpowiednimi licencjami.
34. Mechanizm "antyransomware" musi umożliwiać odtworzenie stanu zasobów urządzenia do wybranego punktu w czasie z okresu nie krótszego niż 30 dni wstecz, z możliwością konfiguracji tego okresu od 1 do 30 dni.
35. Urządzenie musi być objęte serwisem producenta świadczonym w trybie 8x5xNBD przez okres 24 miesięcy od chwili uruchomienia dostarczonej infrastruktury.
36. Wsparcie producenta musi gwarantować Zamawiającemu konkretnego, dedykowanego inżyniera wsparcia poziomu L2 przez cały okres trwania wsparcia. Bezpośrednie informacje kontaktowe do dedykowanego inżyniera (numer telefonu, adres email) umożliwiające uzyskanie wsparcia muszą być dostępne dla Zamawiającego i uaktualniane na bieżąco w razie jego zmiany.