Centrum Edukacji Artystycznej
ul. Mikołaja Kopernika 36/40
00-924 Warszawa
tel. 22 42 10 621
sekretariat@cea.art.pl

Warszawa, dnia 6 grudnia 2024 roku

AG.042.10.2024.LO

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest **„na dostarczenie licencji narzędzia do kompleksowego zarządzania kopiami zapasowymi danych w chmurze, obejmujące zarówno tworzenie i odtwarzanie, jak i administrację systemem na potrzeby Centrum Edukacji Artystycznej”**
2. Opis przedmiotu i zakres zamówienia.

2.1 Główne założenia

2.1.1 Zabezpieczenie danych: rozwiązanie musi zapewniać automatyczne, codzienne tworzenie kopii zapasowych w chmurze następujących elementów: wolumenów danych, stacji roboczych, serwerów wirtualnych.

2.1.2 Kopie zapasowe: proces tworzenia kopii zapasowych powinien być w pełni zautomatyzowany i odbywać się w trybie przyrostowym (incremental backup).
Pierwsza kopia zapasowa: wykonanie pełnej kopii wszystkich danych.
Kolejne kopie: rejestrowanie i zapisywanie wyłącznie zmodyfikowanych plików lub bloków danych od czasu ostatniego backupu, co pozwala na oszczędność przestrzeni dyskowej i czasu operacji.
Kopie pełne: powinny być wykonywane cyklicznie zgodnie z przyjętym harmonogramem (np. raz w tygodniu), w celu zapewnienia spójności i kompletności danych.

2.1.3 Szyfrowanie danych**:** dane powinny być szyfrowane lokalnie (AES-256) przed wysłaniem na serwer docelowy lub chmurę. Klucz szyfrowania pozostaje w gestii użytkownika.

2.2 Wspierane systemy:

2.2.1 możliwość instalacji oraz uruchomienia agenta backupowego na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy: macOS, Windows: 10, Windows 11, Windows Server: 2016 lub nowszy. W środowisk wirtualnych opartych o systemy: Hyper-V, Vmware.

2.2.2 Rozwiązanie umożliwia instalację oraz uruchomienie serwera zarządzania na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy: Windows Client: 10, 11, Windows Server: 2016 lub nowszy.

2.3 Wymagania Data Center

2.3.1 Dwie lub więcej redundantnych serwerowni gwarantujących nieprzerwaną pracę systemu w razie awarii.

2.3.2 Serwerownia zobowiązana jest do utrzymywania przez cały okres trwania umowy parametrów środowiskowych (temperatura, wilgotność) na poziomie zgodnym z zaleceniami producenta sprzętu.

2.3.3 Oferent musi zapewnić łącza internetowe o przepustowości nie mniejszej niż 1 Gb/s dla każdej z głównych lokalizacji serwerowni. Łącza muszą być redundantne, w celu zapewnienia ciągłości działania.

2.3.4 Wymagana jest redundancja w kluczowych elementach infrastruktury, takich jak:

2.3.4.1 Klimatyzacja i systemy chłodzenia.

2.3.4.2 Sieć energetyczna.

2.3.4.3 Łącza telekomunikacyjne.

2.3.5 Serwerownia powinna znajdować się na terenie Polski/UE.

2.3.6 Lokalizacja musi być zgodna z przepisami prawa dotyczącymi przechowywania i przetwarzania danych wrażliwych, w tym wymogami RODO.

2.3.7 Dostęp do serwerowni powinien być zabezpieczony odpowiednimi systemami kontroli dostępu, w tym monitoringiem 24/7.

2.3.8 Serwerownia musi spełniać normy bezpieczeństwa fizycznego i logicznego, takie jak: ISO/IEC 27001 w zakresie zarządzania bezpieczeństwem informacji oraz posiadać odpowiednie certyfikaty potwierdzające standardy jakości infrastruktury.

2.3.9 Gwarancja SLA na poziomie nie niższym niż 99,9% dostępności usług.

2.4 Środowiska fizyczne i bazy danych.

2.4.1 Zadania grupowe: produkt musi umożliwiać tworzenie zadań backupowych zarówno dla grup urządzeń, jak i dla pojedynczych, wybranych urządzeń.

2.4.2 Automatyzacja po zakończeniu backupu: rozwiązanie powinno zapewniać możliwość automatycznego wyłączania stacji roboczych po zakończeniu tworzenia kopii zapasowej.

2.4.3 Obsługa Microsoft SQL: rozwiązanie musi być niezależne od wersji Microsoft SQL i musi umożliwiać przywracanie danych SQL zarówno dla tej samej wersji, jak i dla wersji nowszych.

2.4.4 Odtwarzanie plików: system kopii zapasowej musi wspierać odtwarzanie pojedynczych plików z systemów Windows.

2.4.5 Zarządzanie niedostępnością źródła danych: system powinien oczekiwać na przywrócenie dostępności źródła danych przez czas określony przez administratora. W przypadku dłuższej niedostępności, system musi podejmować określoną przez administratora liczbę prób wznowienia zadania. Po powrocie dostępności danych, system powinien kontynuować backup od momentu przerwania, bez rozpoczynania procesu od początku. Jeśli źródło danych nie stanie się dostępne w wyznaczonym czasie, system powinien zakończyć zadanie z komunikatem o błędzie.

2.4.6 Elastyczność przy odtwarzaniu: odtwarzanie danych musi być możliwe zarówno na sprzęcie identycznym z tym, z którego pochodziły dane, jak i na innym sprzęcie (komputerze lub serwerze). System powinien umożliwiać automatyczne dostosowanie sterowników do nowego sprzętu oraz opcjonalne dodanie sterowników przez użytkownika.

2.4.7 Prawa dostępu przy przywracaniu danych: rozwiązanie musi umożliwiać przywracanie zasobów plikowych zarówno z zachowaniem oryginalnych praw dostępu, jak i bez nich. Konfiguracja tej funkcji powinna być dostępna dla administratora podczas definiowania procesu przywracania danych.

2.5 Środowiska wirtualne.

2.5.1 Wsparcie dla kopii z pełnym kontekstem aplikacyjnym: system musi obsługiwać backup w trybie application-aware dla wszystkich wspieranych platform wirtualizacji, zapewniając integralność danych aplikacji i ich spójność transakcyjną.

2.5.2 Zaawansowane metody transportu: system musi umożliwiać wykonywanie kopii maszyn wirtualnych z zastosowaniem zaawansowanych metod transportu, takich jak HotAdd oraz LAN. Dodatkowo, wymagane jest wsparcie dla metod LAN-Free, które minimalizują obciążenie interfejsów sieciowych maszyn wirtualnych podczas procesu backupu.

2.5.3 Efektywne wykorzystanie zasobów: system kopii zapasowej musi wykorzystywać mechanizmy Change Block Tracking (CBT) oraz ReplicaChangeTracking (RCT) dla wspieranych przez producenta platform wirtualizacji, co pozwala na przyrostowe kopiowanie jedynie zmienionych danych.

2.5.4 Bezpośrednie uruchamianie maszyn wirtualnych z backupu: system musi umożliwiać jednoczesne uruchamianie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i

skompresowanego pliku backupu. Uruchamianie musi być możliwe z dowolnego punktu przywracania, bez konieczności kopiowania danych na produkcyjny magazyn danych. Funkcjonalność ta musi działać w środowiskach VMware niezależnie od rodzaju magazynu danych wykorzystywanego do przechowywania kopii zapasowych.

2.5.5 Elastyczne zarządzanie dyskami: system musi zapewniać możliwość podłączenia pojedynczego dysku bezpośrednio z kopii zapasowej do działającej maszyny wirtualnej w środowisku vSphere.

2.5.6 Weryfikacja spójności danych: system musi umożliwiać automatyczną weryfikację odtwarzalności wirtualnych maszyn zgodnie z harmonogramem ustalonym przez administratora, w dowolnym środowisku, zapewniając regularne testy przywracania danych.

2.6 Bezpieczeństwo.

2.6.1 System plików rozwiązania musi być odporny na ataki ransomware, zapewniając ochronę przed szyfrowaniem end-to-end. Kopie zapasowe nie mogą być nadpisywane – system plików musi być “niezmienny” (immutable).

2.6.2 System powinien umożliwiać odzyskanie hasła głównego administratora w przypadku jego utraty.

2.6.3 Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.

2.6.4 W ramach systemu, komunikacja pomiędzy hostem źródłowym a magazynem danych powinna odbywać się bezpośrednio pomiędzy agentem backupu a magazynem. Komunikacja nie może przechodzić przez serwer backupu ani żaden inny komponent, którego awaria mogłaby sparaliżować działanie systemu. System nie może posiadać pojedynczego punktu awarii (SPOF).

2.7 Administracja rozwiązaniem.

2.7.1 Zakres usługi powinien obejmować:

2.7.1.1 Wsparcie świadczone przez certyfikowanego inżyniera od strony Dostawcy oprogramowania w języku polskim.

2.7.1.2 Pomoc wdrożeniową – pomoc w zaprojektowaniu i wdrożeniu polityk bezpieczeństwa w systemie kopii bezpieczeństwa oraz pomoc w konfiguracji harmonogramów oraz optymalizacji procesów takich jak retencja danych i kompresja.

2.7.1.3 Cotygodniowe monitorowanie usługi SaaS’owej, pomoc w weryfikacji poprawności wykonywanych kopii raz na kwartał po uprzednim umówieniu się na sesję zdalną przez system pomocy Dostawcy. Ewentualny raport z monitoringu oraz poprawności wykonanych kopii powinien być wysyłany na adres email: ….

2.7.1.4 Pomoc w testowym odzyskiwaniu danych, w tym symulacje awaryjnego odtwarzania danych, w celu weryfikacji integralności kopii zapasowych po uprzednim umówieniu się na sesję zdalną przez system pomocy Dostawcy.

2.7.1.5 Priorytet w zgłoszeniach ticketowych - natychmiastowe wsparcie techniczne w przypadku awarii lub problemów z odtwarzaniem danych, z zapewnieniem ciągłości działania usług kopii zapasowych

2.7.2 SLA: Czas reakcji na zgłoszenie incydentu nie przekroczy 4 godzin w godzinach roboczych, a czas rozwiązania problemu zostanie określony indywidualnie dla każdego zgłoszenia.

2.7.3 Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.

2.7.4 Dostawca usługi musi gwarantować brak pojedynczego punktu awarii, zapewniając wysoką dostępność systemu.
2.7.5 Współpraca z dostawcą powinna obejmować:
2.7.5.1 Wsparcie w godzinach roboczych od 7:00 do 16:00.
2.7.5.2 Dostęp do konsoli zarządzającej z uprawnieniami administracyjnymi.
2.7.5.3 Całodobowy dostęp do zgłoszeń ticketowych w sytuacjach krytycznych.
2.7.5.4 Możliwość telefonicznego zgłaszania problemów w dni robocze w godzinach 8:00-16:00.
2.7.6 Dostawca gwarantuje szkolenie z obsługi systemu dla pracowników Zamawiającego z certyfikowanym inżynierem.
2.7.7 Współpraca z lokalnym działem informatycznym Zamawiającego.
2.8 Licencjonowanie i wsparcie techniczne
2.8.1 Wszystkie linie wsparcia muszą być dostępne w języku polskim.
2.8.2 Wsparcie techniczne musi być świadczone przez dostawce rozwiązania.
2.8.3 Dostawca musi zapewnić materiały samopomocowe w języku polskim, w tym dostęp do bazy wiedzy, materiałów wideo oraz kart produktów.
2.8.4 Wsparcie techniczne powinno obejmować połączenia zdalne, system ticketowy oraz wsparcie telefoniczne.
2.8.5 Licencje w ramach rozwiązania powinny pozwalać na zabezpieczenie określonej przez Zamawiającego liczby hostów oraz stacji roboczych w obrębie wspieranych przez system środowisk.
2.8.6 Licencje, przestrzeń chmurowa oraz dostęp do wsparcia technicznego Dostawcy obowiązują przez okres minimum 12 miesięcy (tj. od 01.01.2025 do 31.12.2025).
2.8.7 Sposób licencjonowania: zabezpieczenie 25 stacji roboczych, zabezpieczenie 10 maszyn wirtualnych zlokalizowanych na hostach VMware
2.8.8 Przestrzeń w chmurze o pojemności nie mniejszej niż 4TB. Przestrzeń musi być kompatybilna z proponowanym oprogramowaniem oraz dostępna dla kopii stacji roboczych i maszyn wirtualnych
2.8.9 Dostęp do przestrzeni przeznaczonej dla maszyn wirtualnych musi być ograniczona do publicznego adresu IP Zamawiającego
2.8.10 Przepustowość oraz transfer danych do zdalnego repozytorium nie może być wolniejszy niż 100Mbps.
3 Z wyłonionym Dostawcą rozwiązania, Zamawiający podpisze umowę na dostarczenie narzędzia.