Załącznik nr 1 do Zapytania ofertowego

Nr postępowania: **ZP.271.2.34.2024**

## OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

### I. PRZEDMIOT ZAMÓWIENIA:

**1. Nazwa:** Zakup i dostawa oprogramowania do zautomatyzowanych kopii zapasowych.

**2. Szczegółowy opis przedmiotu zamówienia:**

**Licencje (ilość: 55 sztuk):**

**Zarządzanie i magazyny:**

1. Produkt dostępny w polskiej wersji językowej;

2. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej;

3. System musi umożliwiać tworzenie kopii zapasowych na poziomie dysków;

4. System musi umożliwiać tworzenie kopii zapasowych na poziomie plików i folderów;

5. System musi umożliwiać replikację kopii zapasowych do wielu lokalizacji docelowych;

6. System musi umożliwiać tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT;

7. System musi umożliwiać współpracę z usługą kopiowania woluminów w tle (VSS) firmy Microsoft;

8. Możliwość zdefiniowania limitu przepustowości sieciowej z jakiej ma korzystać oprogramowanie backupowe;

9. System zarządzania nie może być oparty o relacyjne bazy danych;

10. Rozwiązanie musi działać w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie może spowodować przestoju w procesie tworzenia kopii zapasowej);

11. Rozwiązanie musi zapewniać 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);

12. 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;

13. Rozwiązanie musi być systemem multi-storage-owym i umożliwiać tworzenie wielu repozytoriów danych jednocześnie, również na innych środowiskach jako przestrzeń do replikacji danych;

14. System musi oferować mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub być oparty o czas i cykle;

15. System musi pozwalać administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami;

16. 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;

17. Rozwiązanie musi realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie;

18. Rozwiązanie musi zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia;

19. System musi umożliwiać automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku wystąpienia błędu;

20. Rozwiązanie powinno umożliwiać klonowanie planów kopii zapasowych, planów replikacji oraz planów testowego odtwarzania maszyn wirtualnych;

21. Rozwiązanie powinno umożliwiać uruchamianie przy zadaniach backupu dowolnych skryptów PRE/POST oraz po wykonaniu migawki VSS;

22. System powinien umożliwiać definiowanie tzw. okna backupowego dla każdego z zadań w celu umożliwienia zarządzania obciążeniem sieci i uwzględnienia okien serwisowych występujących u Zamawiającego;

23. System musi automatycznie dodawać do polityki i harmonogramu tworzenia backupów nowe źródła/maszyny wirtualnych, dodane do bieżącego środowiska (automatyzacja oparta na polityce tworzenia kopii);

24. 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;

25. 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;

26. System powinien umożliwiać wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika;

27. Oferowane rozwiązanie musi być dobrane pod względem wydajności w oparciu o najlepsze praktyki producenta;

28. 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 Przedmiotu Zamówienia;

29. 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);

30. System musi pozwalać 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;

31. Proces deduplikacji musi być możliwy dla każdego z typów obsługiwanych magazynów;

32. Proces deduplikacji nie może wymagać instalacji żadnych dodatkowych komponentów, które będą pośredniczyły w zapisie danych z deduplikowanych;

33. Proces deduplikacji nie może posiadać pojedynczego punktu awarii;

34. Proces deduplikacji musi być realizowany blokiem o stałej wielkości;

35. Proces szyfrowania kopii zapasowych nie może ograniczać procesu deduplikacji w ramach tego samego klucza szyfrującego;

36. Kompresja kopii zapasowych musi obsługiwać jeden z wymienionych algorytmów: LZ4, ZStandard. Dodatkowo, musi umożliwiać określenie szczegółowego poziomu kompresji, w tym: niski, średni, wysoki;

37. Instalacja, modyfikacja ustawień, polityki tworzenia kopii zapasowej systemu nie może wymagać przerwania pracy lub restartu systemu;

38. System musi pozwalać na automatyczne aktualizacje oprogramowania;

39. System musi być w stanie kompresować i szyfrować zabezpieczone dane w systemach NAS;

40. System musi pozwalać na uruchomienie kontenerów Docker w dowolnych urządzeniach NAS w celu ich zabezpieczenia;

41. System zarówno musi przechowywać dane w kopii zapasowej w postaci zaszyfrowanej jak też ruch wewnątrz systemu musi być szyfrowany;

42. Archiwum długoterminowych kopii zapasowych musi być szyfrowane, a odzyskiwanie z archiwum obsługiwane z tego samego interfejsu użytkownika, co inne przywracane dane;

43. System musi mieć mechanizmy chroniące przejęcie konta administratora oraz umożliwiać definiowanie dodatkowych uprawnień dla każdej z predefiniowanych ról użytkowników;

44. System musi pozwalać na gradację uprawnień administratorów - umożliwiać 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;

45. Rozwiązanie musi posiadać możliwość nieodwracalnego usuwania danych z magazynu na dane w momencie spełnienia dodatkowych wymogów;

46. 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;

47. 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;

48. System kopii zapasowej musi umożliwiać dostęp do konsoli administracyjnej z wielu stacji roboczych;

49. System kopii zapasowej musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych;

50. System powinien posiadać predefiniowany schemat tworzenia kopii zapasowych: G-F-S, Forever incremental;

51. Rozwiązanie musi obsługiwać kontrolę dostępu opartą na rolach (RBAC);

52. Możliwość składowania utworzonych kopii zapasowych na magazynach chmurowych: Amazon AWS, Azure, Wasabi, Google Cloud Storage, Backblaze B2, magazyny zgodne z S3;

53. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych po protokole smb, nfs, iscsi, katalog lokalny;

54. 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);

55. 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;

56. Możliwość generowania raportów dobowych w oparciu o harmonogram;

57. Produkt musi posiadać możliwość zapisu kopii zapasowych do magazynu chmurowego dostarczanego bezpośrednio przez producenta oprogramowania (datacenter musi być zlokalizowane na terenie UE);

58. 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);

59. Możliwość wyświetlenia szczegółowych informacji o chronionym urządzeniu takich jak: CPU, RAM, System operacyjny, Adres IP;

60. Produkt musi posiadać możliwość zdefiniowania poziomu obciążenia magazynu, po osiągnięciu którego zostanie wysłane powiadomienie e-mail (poziom definiowany indywidualnie dla każdego magazynu).

**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 m.in.: BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption;

5. System musi być 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. 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;

9. Rozwiązanie powinno umożliwiać uruchamianie procesu Bare Metal Restore z dowolnego bootowalnego nośnika danych;

10. Rozwiązanie powinno wspierać odtwarzanie danych w scenariuszach: P2P, P2V, V2P, V2V;

11. Rozwiązanie powinno umożliwiać odtwarzanie kopii obrazu dysku w wybranym formacie (RAW, VHD, VHDX, VMDK);

12. 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;

13. Rozwiązanie musi umożliwiać przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows).

**Środowiska wirtualne:**

1. System musi wspierać kopię w trybie application-aware dla wszystkich wspieranych wirtualizatorów;

2. System musi umożliwiać wykonywanie kopii maszyn wirtualnych z zastosowaniem 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.

**Aplikacje SaaS:**

1. Ochrona z tej samej konsoli dla Microsoft 365 minimum 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;

5. System musi umożliwiać zabezpieczanie środowisk Jira.

**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 menadżera 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.

**Licencjonowanie i wsparcie techniczne:**

1. Wszystkie linie supportu muszą być obsługiwane w języku polskim;

2. Wsparcie techniczne musi być świadczone bezpośrednio przez główną siedzibę producenta;

3. Możliwość zgłaszania ticketów supportowych przez formularz zgłoszeniowy znajdujący się na oficjalnej stronie www producenta;

4. Producent wraz z rozwiązaniem musi udostępnić materiały samopomocowe w języku 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. Licencje powinny być dostępne w opcji wieczystej. Wsparcie techniczne nie powinno być wymagane dla poprawnego działania systemu;

7. Dostęp do wsparcia technicznego producenta powinien obowiązywać przez okres min. 24 miesięcy;

8. Sposób licencjonowania opiera się na:

- ilości serwerów/endpointów - dla fizycznych urządzeń,

- ilości fizycznych hostów - dla środowisk wirtualnych,

- ilości repozytoriów - dla GIT,

- ilości userów - dla Jira,

- ilości maszyn wirtualnych (opcja dodatkowa);

9. Licencje powinny umożliwiać zabezpieczenie w wersji wieczystej - 55 stacji roboczych.

**Wdrożenie:**

1. Wdrożenie musi się odbyć w formie zdalnej;

2. Wdrożenie musi zostać przeprowadzone bezpośrednio przez producenta oprogramowania lub przez certyfikowanego producenta inżyniera;

3. Wdrożenie musi się odbyć w języku polskim;

4. Wdrożenie musi obejmować podstawowe szkolenie z obsługi oprogramowania;

5. Czas wdrożenia – 8 godzin;

6. Wdrożenie zakończone jest szkoleniem z obsługi oprogramowania.

**Szkolenie:**

1. Szkolenie realizowane jest bezpośrednio przez producenta oprogramowania lub przez certyfikowanego producenta trenera;

2. Szkolenie realizowane jest w formie zdalnej;

3. Komunikacja podczas szkolenia musi odbywać się w języku polskim;

4. Czas szkolenia – 8 godzin;

5. Szkolenie musi zakończyć się imiennym certyfikatem dla każdego z uczestników.

**3. Termin realizacji (dostawy) przedmiotu zamówienia**: 30 dni od dnia udzielenia zamówienia (od dnia wystawienia zlecenia).

**4.** Zamawiający nie dopuszcza składania ofert częściowych.

**5.** Zamawiający nie dopuszcza składania ofert wariantowych.

**6.** Przedmiot zamówienia jest realizowany w związku z:

**Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC)**

**Priorytet II: Zaawansowane usługi cyfrowe**

**Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa**

**konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd” o numerze FERC.02.02-CS.01-001/23**.

**II. WYMAGANE DOKUMENTY, KTÓRE ZOBOWIĄZANY BĘDZIE ZŁOŻYĆ WYKONAWCA:**

1) Formularz oferty (wg załączonego wzoru) – załącznik nr 2 do zapytania ofertowego;

2) Oświadczenie Wykonawcy – załącznik nr 4 do zapytania ofertowego;

3) Odpis lub informacja z Rejestru Przedsiębiorców Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej Rzeczypospolitej Polskiej, w zakresie art. 109 ust. 1 pkt 4 ustawy Pzp, sporządzonych nie wcześniej niż 3 miesiące przed jej złożeniem, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji.

**III. WSPÓLNY SŁOWNIK ZAMÓWIEŃ (CPV):**

CPV: 48710000-8 - Pakiety oprogramowania do kopii zapasowych i odzyskiwania.

**IV. KRYTERIUM OCENY OFERT:** Cena brutto oferty (waga-100 %).

Klembów, dnia 18.10.2024 r.

*/-/Rafał Mathiak*
*Wójt Gminy Klembów*

.....
(Data i podpis Kierownika Zamawiającego lub osoby upoważnionej)