OPIS PRZEDMIOTU ZAMÓWIENIA

1. **Przedmiot zamówienia**
   1.1. Przedmiotem zamówienia jest świadczenie usługi wsparcia technicznego dla środowiska kopii zapasowych na zasadach oprogramowania producenta, opartych o aplikację Commvault 11 (zwanych dalej „usługą wsparcia technicznego").
   1.2. Świadczenie usługi Wsparcia Eksperckiego w ilości 80 roboczogodzin, którego zakres został opisany w punkcie 5.4
2. **Termin realizacji / okres obowiązywania**
   2.1. Termin realizacji zamówienia nie wcześniej niż od 06.12.2026.
   2.2. Okres obowiązywania świadczenia usługi wsparcia technicznego i usługi wsparcia eksperckiego na okres 24 miesięcy.
3. **Zakres zamówienia podstawowego**

Zakres zamówienia podstawowego obejmuje:

3.1. Świadczenie usług wsparcia technicznego. (nie wcześniej niż od dnia 6 grudnia 2026, w odniesieniu do licencji posiadanych przez Zamawiającego opisanych w punkcie 5.2.

3.2. Zapewnienie Wsparcia Eksperckiego w ilości 80 roboczogodzin, zgodnie z pkt 5.4. niniejszego OPZ.

4. **Wymagania ogólne**

Świadczone Usługi muszą:

4.1. Być realizowane z należytą starannością, zgodnie z najlepszą wiedzą techniczną i obowiązującymi standardami branżowymi.
4.2. Być realizowane przez osoby posiadające adekwatnych do przedmiotu zamówienia kwalifikacje, doświadczenie i uprawnienia.
4.3. Nie powodować zakłóceń w pracy systemów i infrastruktury Zamawiającego.
4.4. Być realizowane w sposób zapewniający bezpieczeństwo informacji i danych Zamawiającego.
4.5. Być zgodne z obowiązującymi przepisami prawa, w tym dotyczącymi ochrony danych osobowych.

5. **Wymagania funkcjonalne / merytoryczne**

5.1. Kopie zapasowe środowiska Zamawiającego są wykonywane przez system Commvault 11. Obecnie w systemie kopii zapasowych wykorzystane są następujące licencje:

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

- licencja Commvault Complete Backup & Recovery for Virtualized Environments, Per Socket. Perpetual CV-BR-SK – (CPU Sockets on Hypervisor Hosts), – 112 sztuk;
- licencja Commvault Complete Backup & Recovery for Physical Servers, Per OperatingInstance CV-BR-O - 40 sztuk;
- CV-BR-MB, CVLT Complete Backup & Recovery for Mailboxes & Cloud Apps, Per User – 1300 szt.

Środowisko systemu kopii zapasowych i archiwizacji Zamawiającego wykonuje kopie maszyn wirtualnych (VMWare, HyperV) z systemami operacyjnymi z rodzin MS Windows i Linux, baz danych typu MS-SQL, Postgress, DB2, Oracle, Sharepoint i aplikacji Redmine, Docker, Kubernetes, Jboss, Office365.

5.2. Wsparcie techniczne obejmuje bieżące usuwanie awarii, konfigurację systemów oraz zdalne konsultacje w przypadku problemów z działaniem oprogramowania oraz dostęp do najnowszych aktualizacji producenta, opartych o aplikację Commvault 11

5.3. Wykonawca w ciągu 5 dni roboczych dostarczy Zamawiającemu dokument wystawiony przez producenta oprogramowania, potwierdzający możliwość korzystania z Usługi przez Zamawiającego.

5.4. Zamawiający wymaga, aby Usługa Wsparcia Eksperckiego była świadczona przez minimum dwóch pracowników posiadających certyfikat CommVault Certified Engineer (lub równoważny) oraz dodatkowo co najmniej jednego posiadającego certyfikat CommVault Certified Expert (lub równoważny)

5.5. Wykonawca zapewni personel spełniający wymagania podany w punkcie 5.2

5.6. Wykonawca będzie świadczył usługę wsparcia eksperckiego w wymiarze 80 roboczogodzin w okresie obowiązywania umowy, tj. od zawarcia umowy, lecz nie wcześniej niż od dnia 6 grudnia 2026. obejmujące:

a. wsparcie przy aktualizacji środowiska kopii zapasowych,
b. przeglądy środowiska obejmujące weryfikację poprawności instalacji, konfiguracji i działania systemu kopii zapasowych,
c. konsultacje i doradztwo w zakresie eksploatacji środowiska oraz jego bezpieczeństwa,
d. konsultacje w ramach rozwoju środowiska pod kątem obejmowania kopiami zapasowymi nowych systemów Zamawiającego,
e. konsultacje implementacji nowych, nietypowych oraz dostosowywania już istniejących metod optymalizacji systemów Zamawiającego w zakresie funkcjonalności oferowanej przez środowisko.
f. inne prace wg. potrzeb Zamawiającego (w uzgodnieniu z Wykonawcą).

6. Rozwiązania równoważne

6.1. Jeżeli w OPZ wskazano nazwy własne, technologie, metodyki lub standardy, należy je rozumieć jako odniesienia przykładowe.

6.2. Zamawiający dopuszcza realizację Usług w sposób równoważny, spełniający co najmniej wszystkie wymagania OPZ.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

6.3. Wykonawca zobowiązany jest wykazać równoważność sposobu realizacji Usług.
6.4. Niewykazanie równoważności skutkuje uznaniem, że oferta nie spełnia wymagań OPZ.
6.5. Zamawiający dopuszcza zaoferowanie produktów równoważnych do oprogramowania dla licencji Commvault Cloud Autonomous Recovery Software for Virtual Machines, Per VM.
6.6. W przypadku dostarczania oprogramowania równoważnego względem wyspecyfikowanego przez Zamawiającego w Opisie przedmiotu zamówienia, Wykonawca musi na swoją odpowiedzialność i swój koszt udowodnić, że dostarczane oprogramowanie spełnia wszystkie wymagania i warunki określone w Opisie Przedmiotu Zamówienia, w szczególności w zakresie:
    6.6.1. dostarczone licencje/ sublicencje w każdym aspekcie licencjonowania / sublicencjonowania, muszą być identyczne lub rozszerzone, przy czym rozszerzony zakres musi zawierać również wszystkie elementy licencjonowania jak dla oprogramowania Commvault
    6.6.2. funkcjonalności równoważnej oprogramowania, która nie może być gorsza od funkcjonalności wymienionych w pkt V „Opis wymaganych minimalnych funkcjonalności w przypadku zaoferowania oprogramowania równoważnego …”,
6.7. oprogramowanie równoważne musi być kompatybilne i w sposób niezakłócony współdziałać z oprogramowaniem Commvault funkcjonującym u Zamawiającego,
6.8. oprogramowanie równoważne musi posiadać pełne wsparcie dla backupu systemów opartych o środowiska systemowo-programowalne Zamawiającego, wymienione w punkcie 5.3.,
6.9. oprogramowanie równoważne nie może zakłócać pracy systemów Zamawiającego, opartych o dotychczas użytkowane oprogramowanie backupowe Commvault,
6.10. oprogramowanie równoważne musi zapewniać pełną, równoległą współpracę w czasie rzeczywistym i pełną funkcjonalną zamienność oprogramowania równoważnego z wyspecyfikowanym oprogramowaniem,
6.11. W przypadku dostarczenia rozwiązania równoważnego Wykonawca musi wymienić posiadany przez Zamawiającego system kopii zapasowych na oferowany. W tym celu Wykonawca musi skonfigurować zadania kopii zapasowych, przenieść ich specyfikację oraz harmonogramy, przeprowadzić testy odtworzeniowe oraz dostarczyć wymagany sprzęt wraz z systemem operacyjnym oraz niezbędne licencje.
6.12. W przypadku zaoferowania przez Wykonawcę oprogramowania równoważnego Wykonawca dokona transferu wiedzy w zakresie utrzymania i rozwoju rozwiązania opartego o zaproponowane oprogramowanie
6.13. w przypadku, gdy zaoferowane przez Wykonawcę oprogramowanie równoważne nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego i/lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego również po usunięciu oprogramowania równoważnego.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

6.14. Oprogramowanie równoważne dostarczane przez Wykonawcę nie może powodować utraty kompatybilności oraz wsparcia producentów używanego i współpracującego z nim oprogramowania u Zamawiającego

6.15. Oprogramowanie równoważne zastosowane przez Wykonawcę nie może w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest zastosowanie oprogramowania równoważnego, dla którego producent ogłosił zakończenie jego rozwoju w terminie 3 lat licząc od momentu złożenia oferty. Niedopuszczalne jest użycie oprogramowania równoważnego, dla którego producent oprogramowania współpracującego ogłosił zaprzestanie wsparcia w jego nowszych wersjach.

6.16. W przypadku dostawy oprogramowania równoważnego Wykonawca zobowiązany jest:

6.17. Przeprowadzić Instruktaż dla 6 administratorów Zamawiającego z zakresu instalacji, konfiguracji i zarządzania oprogramowaniem równoważnym, umożliwiającym pełne poznanie produktu równoważnego. Wykonawca w terminie 1 dnia roboczego od dnia zawarcia Umowy przedstawi do zatwierdzenia Zamawiającemu harmonogram Instruktażu. Instruktaż będzie realizowany w dni robocze w godzinach 8:00-16:00 w siedzibie Zamawiającego lub w formie zdalnej o ile zostaną spełnione wszystkie wymagania dotyczące Instruktażu. Instruktaż będzie trwał minimum 2 dni robocze (łącznie minimum 14 godzin zegarowych).

6.18. Zainstalować oprogramowanie równoważne w środowisku systemowo-programowym w terminie do 5 dni roboczych od dnia podpisania Umowy.

6.19. Dostarczyć wszelkich dodatkowych licencji - niezbędnych do prawidłowego funkcjonowania oprogramowania równoważnego.

6.20. Wykonawca oferujący Oprogramowanie równoważne zobowiązany jest wykazać spełnienie wymagań równoważności poprzez złożenie wraz z ofertą dokumentów umożliwiających ocenę zgodności oferowanego rozwiązania z OPZ.W szczególności Wykonawca zobowiązany jest do przedłożenia:

a) tabeli zgodności, obejmującej:
-numer i treść każdego wymagania określonego w OPZ,
-opis sposobu spełnienia danego wymagania przez oferowane rozwiązanie,
-wskazanie dokumentu potwierdzającego spełnienie wymagania (nazwa dokumentu, numer strony lub sekcji),
-link do oficjalnego źródła producenta – jeżeli dotyczy;
b) dokumentów producenta oferowanego Oprogramowania, potwierdzających spełnienie wymagań, w szczególności kart katalogowych, oficjalnych list kompatybilności, certyfikatów oraz dokumentacji technicznej, pochodzących bezpośrednio od producenta lub z jego oficjalnych repozytoriów.

6.21. Dokumenty potwierdzające spełnienie wymagań równoważności mogą być złożone w języku polskim lub angielskim.

6.22. Na wezwanie Zamawiającego Wykonawca zobowiązany jest do przedstawienia dodatkowych wyjaśnień, uzupełnień lub dokumentów potwierdzających spełnienie wymagań równoważności.

6.23. Niewykazanie spełnienia któregokolwiek z wymagań określonych w OPZ skutkować będzie uznaniem, że oferowane Oprogramowanie nie spełnia wymagań Zamawiającego.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

6.24. Wszelkie koszty, ryzyka oraz działania techniczne i organizacyjne związane z zapewnieniem równoważności, w tym integracją, migracją, dostosowaniem lub przywróceniem prawidłowego działania środowiska Zamawiającego, obciążają Wykonawcę.

6.25. Opis wymaganych minimalnych funkcjonalności w przypadku zaoferowania oprogramowania równoważnego w stosunku do oprogramowania do archiwizacji kopii zapasowych dla licencji Commvault Cloud Autonomous Recovery Software for Virtual Machines, Per VM.

6.26. Rozwiązanie równoważne (dalej: System) musi reprezentować architekturę trójwarstwową (serwer zarządzający, serwer medialny oraz klient), taka architektura pozwoli na elastyczną skalowalność rozwiązania bez względu na dynamikę przyrostu danych.

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

6.28. Jeśli rozwiązanie równoważne korzysta z bazy danych to wszelkie potrzebne licencje muszą być dostarczone i stanowić całość oferty, z tym, iż licencje dla silnika bazodanowego muszą pozwalać na zainstalowanie go: na serwerze fizyczny (minimum 2xCPU po 16 core), klastrze active-passive czy serwerze wirtualnym w środowisku Vmware i Hyper-V.

6.29. Licencje muszą pozwalać na stworzenie dla serwera zarządzającego rozwiązania wysokodostępnego z częstotliwością replikacji bazy katalogowej nie dłuższym niż 15 minut (RPO nie większe niż 15 minut dla uruchomienia zapasowego serwera zarządzającego). Jeśli do stworzenia takowego rozwiązania potrzebne są licencje replikacyjne, klastrowe, współdzielona przestrzeń dyskowa to muszą zostać zaoferowane. Licencje muszą pozwalać na skonfigurowanie serwerów zarządzających oraz ich replikację dla co najmniej trzech lokalizacji, gdzie pierwsza jest lokalizacja produkcyjna, druga i trzecia są typu standby dla serwera zarządzającego.

6.30. Musi istnieć możliwość zainstalowania serwera zarządzającego na systemie operacyjnym Linux z zachowaniem możliwości replikacji bazy katalogowej i tworzeniem serwerów typu standby.

6.31. Rozwiązanie równoważne musi zapewnić interfejs graficzny do zarządzania i instalacji.

6.32. Oprogramowanie musi umożliwiać zdalne instalowanie i odinstalowywanie klienta system z centralnego serwera dla systemów Windows, Linux i Unix – musi być to możliwe z jednego serwera pełniącego rolę cache dla wszystkich binarii klienckich.

6.33. System musi zapewniać funkcjonalność odtwarzania po awarii konfiguracji serwera zarządzającego tworzeniem kopii bezpieczeństwa i archiwów.

6.34. Zaproponowane równoważne rozwiązanie musi wspierać backup całych maszyn wirtualnych/kontenerów dla czołowych rozwiązań wirtualizacyjnych, kontenerowych i chmurowych:

- Amazon
- Microsoft Azure
- Microsoft Azure Stack Hub
- Microsoft Azure Stack HCI
- Microsoft Hyper-V

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

- Kubernetes
- Oracle Cloud Classic
- Oracle Cloud Infrastructure
- Oracle VM
- Red Hat OpenShift
- Red Hat Virtualization
- vCloud Director
- VMware

6.35. Musi posiadać dedykowany komponent do backupu minimum całej maszyny wirtualnej/kontenera/aplikacji/wolumenu bez konieczności instalowania agenta wewnątrz np. maszyny z możliwością granualnego odtwarzania pojedynczych plików.

6.36. Dla maszyn wirtualnych musi być możliwość zainstalowania agenta plikowego i bazodanowego dla zabezpieczenia zasobów z wewnątrz maszyny wirtualnej – funkcjonalność ta musi być zawarta dla wszystkich wymaganach wirtualizatorów i być w cenie rozwiązania.

6.37. Przy odtwarzaniu danych środowisk kontenerowych musi istnieć możliwość selekcji zasobów podlegającym odtworzeniu

6.38. Dla backupu i odtwarzania środowisk wirtualnych opartych o Vmware musi być możliwość wyboru różnych transportów: SAN, Hot-add, NBD, SSL, NAS - gdzie transport NAS pozwala na bezpośredni odczyt i zapis danych maszyny wirtualnej z urządzenia NAS

6.39. System musi zapewniać automatyczne wykrywanie i dodawanie do polityki backupu nowych maszyn wirtualnych.

6.40. System musi umożliwiać odzyskanie i uruchomienie maszyn wirtualnych z kopii zapasowej bez oczekiwania na pełne przywrócenie maszyny wirtualnej minimum dla Vmware i Hyper-V.

6.41. System musi umożliwiać konwertowanie maszyn wirtualnych pomiędzy wirtualizatorami, minimum:

- Vmware do: Hyper-V, Azure, Amazon, Openstack, Oracle Cloud Infrastructure
- Hyper-V do: Azure, Amazon, Vmware
- Amazon do: Azure, Vmware
- Azure do: Amazon, Hyper-V, Vmware

Co oznacza, iż w przypadku odtwarzania zbackupowanej maszyny wirtualnej istnieje możliwość wybrania innego wirtualizatora jako miejsce odtwarzania i uruchomienia odtworzonej maszyny wirtualnej.

6.42. System musi wspierać mechanizm CBT (change block tracking) minimum dla Vmware i Hyper-V

6.43. System musi umożliwiać konwersję zbackupowanego serwera Windows i Linux do maszyny wirtualnej w środowisku: Hyper-V; Vmware

6.44. Możliwość synchronizacji maszyn wirtualnych Vmware do środowiska Hyper-V, Vmware celem budowy rozwiązania DR (Disaster Recovery) z funkcjonalnościami:

- Failover (planowane i niezaplanowane/awaryjne)
- Failback

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

6.45. System (jako opcja) musi oferować rozbudowę o funkcjonalność przeszukiwania i analizy zasobów plikowych dla maszyn wirtualnych (minimum Vmware) całość działać związanych musi odbywać się na kopiach backupowych maszyn wirtualnych a nie na środowisku produkcyjnym

6.46. System musi posiadać możliwość nieodwracalnego kasowania danych – funkcjonalność ta musi być częścią oprogramowania i musi pozwalać na wyczyszczenie przestrzeni dyskowych (zamazanie) tak aby narzędziami niskiego poziomu nie było możliwości odzyskania tych danych.

6.47. Administrator systemu musi mieć możliwość wybrania (minimum) plików z danej kopii backupowej i ich skasowania, tak aby nie było możliwości ich późniejszego odtworzenia z tej kopii.

6.48. 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.

6.49. System musi pozwalać na składowanie danych na taśmach celem przechowywania długoterminowego. Składowane dane na taśmach muszą być w formie nie zdeduplikowanej (nawodnione) po to by była możliwość odtwarzania ich bezpośrednio, a więc bez konieczności pośrednictwa dysków, buforów czy importu.

6.50. System musi pozwalać na zarządzanie całością działania systemu (backup, archiwizacja, backup laptopów) z jednej konsoli administracyjnej.

6.51. Agenci systemu muszą posiadać funkcjonalność komunikowania się poprzez jeden port TCP/IP, celem zabezpieczenia komunikacji z środowisk typu DMZ.

6.52. Automatyczne tunelowanie komunikacji TCP/IP pomiędzy agentami systemu – jeśli agent systemu wykryje ograniczenia w komunikacji, wówczas automatycznie zestawia połączenie tunelowe wykorzystujące tylko jeden port TCP/IP.

6.53. System musi umożliwiać nie tylko szyfrowanie danych (kopii backupowych) ale także całej komunikacji pomiędzy komponentami systemu (minimum pomiędzy agentem backupowym a serwerem składującym i zarządzającym kopiami).

6.54. System musi umożliwiać konfigurację, którymi kartami sieciowymi ma przebiegać komunikacja i transfer danych, wybór interface musi odbywać się co najmniej poprzez nazwę domeny, subnet, zakres IP.

6.55. System musi pozwalać na współdzielenie napędów taśmowych w środowisku sieci SAN.

6.56. System musi umożliwić przechowywanie jedynie unikalnych bloków danych tzw. deduplikacja. Funkcjonalność ta musi działać na poziomie blokowym i być wykonywana online podczas procesu tworzenia kopii danych. Deduplikacja musi być realizowana poprzez oprogramowanie system na dowolnym sprzęcie czy to w warstwie serwera systemu czy klienta. Pojedynczy serwer systemu musi umożliwiać przechowywanie danych po deduplikacji minimum do 500 TB (rozbudowa do tej wielkości może nastąpić tylko poprzez dodanie dodatkowej przestrzeni do składowania danych poprzez dodanie dysków, półki dyskowej a nie przez wymianę urządzenia czy serwera).

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

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

6.58. Logiczna Globalna deduplikacja – system musi oferować deduplikację globalną co oznacza, iż niezależnie z jakich klientów dane będą deduplikowane (serwery fizyczne, hosty wirtualne, bazy i aplikację) – deduplikacja musi opierać się na jednej logicznej centralnej bazie deduplikacyjnej.

6.59. Włączenie funkcjonalności deduplikacji nie może generować wymogu instalacji dodatkowych modułów programowych po stronie klienckiej lub serwera systemu. Niedopuszczalne jest łączenie systemu z dodatkowym oprogramowaniem czy sprzętem (appliance) dla uzyskania funkcjonalności deduplikacji danych.

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

6.61. System musi zapewniać wspólny stopień deduplikacji (jedna baza deduplikacyjna) dla danych czy to z backupu czy archiwizacji.

6.62. System musi umożliwiać wykonywanie kopii w post procesie do drugiej lokalizacji przesyłając jedynie unikalne bloki danych (dla dowolnych danych: czy to z procesu backupu czy archiwizacji). A więc replikacja danych do innej lokalizacji musi być wykonywana na danych po deduplikacji i funkcjonalność ta musi być realizowana i zarządzana z poziomu systemu.

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

6.64. System musi składować dane po deduplikacji (kopie backupowe) na storage obiektowym zgodnym z S3 czy to w środowisku onpremis czy cloud, musi wspierać technologię WORM na tych typach storage, transfer danych musi odbywać się z wykorzystaniem deduplikacji i muszą być wysyłane tylko unikalne bloki danych. Nie dopuszczalne jest, aby tworzenie kolejnej kopii danych na storage obiektowym wymagało nawodnienia danych – transfer musi odbywać się tylko unikalnych bloków danych.

6.65. System musi pozwalać na instalację bazy deduplikacyjnej w układzie wysokiej dostępności (minimum na dwóch serwerach) w taki sposób, aby awaria pojedynczego serwera nie powodowała utraty możliwości backupu z deduplikacją i odtwarzania wcześniejszych kopii danych.

6.66. System musi pozwalać na odtwarzanie zdeduplikowanych danych nawet w momencie, gdy baza deduplikacyjna jest niedostępna. Proces odtwarzania (nawadniania) zdeduplikowanych danych nie korzysta z bazy deduplikacyjnej.

6.67. Na jednym serwerze systemu (na jednej instancji systemu operacyjnego) może być zainstalowane minimum dwie bazy deduplikacyjne pozwalające zwiększyć skalowalność systemu.

6.68. System musi zapewniać dostęp zintegrowany z usługą katalogową, minimum Active Directory, a więc tak zwany „single sign on” – pojedyncze logowanie: użytkownik po zalogowaniu do domeny AD, nie potrzebuje wykonywać następnego logowani, aby zarządzać systemem poprzez konsolę administracyjną.

6.69. Możliwość uruchomienia logowania wieloskładnikowego (MFA) dla dostępu do konsoli administracyjnej.

6.70. System musi być odporny na tzw. „atak na wzorzec czasu”: to znaczy, iż przy radykalnej zmianie czasu na serwerze zarządzającym System musi automatycznie zatrzymać co najmniej proces

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

kasowania (ekspiracji) kopii backupowych generując odpowiednie alerty do czasu potwierdzenia tej zmiany przez administratora.

6.71. System musi zapewniać elastyczne delegowanie uprawnień oraz audytowanie działań użytkowników. Z tym, że 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.

6.72. Komunikacja pomiędzy agentem a serwerem systemu musi opierać się na certyfikatach

6.73. System musi posiadać funkcjonalność blokowania danych do odczytu dla administratora, to znaczy, że administrator systemu nawet mając pełne uprawnienia nie może odtworzyć danych, jeśli nie jest ich właścicielem, funkcjonalność ta musi być dostępna i minimum dla danych z laptopów/desktopów.

6.74. System musi pozwalać na skonfigurowanie mechanizmu podwójnej autentyfikacji (MPA) administratora – do uruchomienia konsoli administracyjnej systemu potrzebne jest nie tylko logowanie, ale i dodatkowy tymczasowy kod wysyłany do administratora np. poprzez mail.

6.75. Szyfrowanie danych musi pozwalać na wybór algorytmu (minimum dwa algorytmy: Blowfish, AES) także dla danych deduplikowanych na kliencie systemu.

6.76. 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.

6.77. System musi wspierać mechanizm szyfrowania danych na napędach taśmowych LTO.

6.78. System musi mieć wbudowane mechanizmy zabezpieczające przed złośliwym oprogramowaniem (Ransomware), minimum:

a) Dedykowany dashboard będący częścią konsoli administracyjnej systemu do identyfikacji i zarządzania zagrożeniami, pozwalający administratorowi na działania proaktywne lub reaktywne w momencie wykrycia zagrożenia.

b) Monitorowanie nietypowych zachowań systemu backupowego obejmującego obszary:

- Czyszczenia bazy deduplikacyjnej (DDB)
- Zadarzeń w Systemie (events)
- Ilości nieudanych zadań
- Ilości zadań czekających
- Ilości zadań zakończonych sukcesem
- Konsoli monitorującej zadania
- Czasu trwania zadań.

6.79. Zabezpieczenie ścieżek dostępu do danych składowanych (kopii backupowych) na dyskach – tylko procesy systemu mogą zapisywać i modyfikować dane.

6.80. Monitorowanie (jako opcja) nietypowych aktywności na serwerach plikowych.

6.81. Monitorowanie nietypowych aktywności na serwerach za pomocą metody: Honeypot (plików pułapek/wabików) – system cyklicznie i automatycznie sprawdza czy pliki pułapki nie były modyfikowane.

6.82. Monitorowanie (jako opcja) możliwego zagrożenia dotyczącego zaszyfrowania plików na serwerach.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

6.83. Monitorowanie (jako opcja) różnych typów plików i weryfikowanie czy typ pliku jest zgodny i czytelny z nagłówkiem tego pliku (detekcja uszkodzeń plików czy ich zaszyfrowania).

6.84. Monitorowanie klientów Systemu i alertowanie o tych, którzy tracą komunikację z Systemem Air Gap (izolowanie i segmentowanie składowanych kopii backupowych) – musi polegać na wbudowanym automatycznym mechanizmie wyłączania komunikacji pomiędzy pozostałymi komponentami systemu backupowego. Tak więc komunikacja z wybranym segmentem środowiska backupowego odbywa się tylko w określonym przedziale czasowym dla potrzeb replikacji kopii backupowych, natomiast przez pozostały czas żadne procesy systemu backupowego nie mają możliwości komunikacji z tym środowiskiem.

6.85. Możliwość definiowania serwerów komunikacyjnych (tzw. bram/gateway) przez które wykonywana jest komunikacja pomiędzy modułami systemu backupowego, w szczególności pomiędzy serwerem zarządzającym a serwerem medii czy serwerem z dowolnym agentem backupowym.

6.86. Możliwość definiowania kierunku inicjalizowania komunikacji sieciowej pomiędzy komponentami systemu backupowego.

6.87. Mechanizm WORM - możliwość zablokowania zmiany retencji (czas przechowywania kopii backupowych) na krótszą dla kopii backupowych składowanych na dowolnych typach nośników w tym na dyskach i taśmach.

6.88. Wsparcie dla mechanizmu WORM dla macierzy obiektowych min: Hitachi Vantara HCP i storage obiektowego w chmurze minimum: Azure, AWS, Google.

6.89. MFA (Multi Factor Authentication) - uwierzytelnianie wieloskładnikowe.

6.90. MPA (Multi Person Autorysation) – dwuosobowa autoryzacja działań (w przypadku wykonywania przez administratora systemu działania, które spowoduje skasowanie danych inna/dodatkowa osoba musi potwierdzić lub odrzucić takie działanie).

6.91. Wszelkie działania w systemie, także działania użytkowników końcowych muszą być logowane i przechowywane.

6.92. System musi posiadać zaawansowane mechanizmy exportu i analizy logów poprzez:

- Syslog serwer.
- Splunk (dedykowany plug-in do Spluk dla analizy danych).

6.93. System musi posiadać rozbudowany system raportowania dla administratorów, minimalny zestaw dostępnych raportów to:

a) Raport zmian/wzrostu środowiska system
b) Raport wykorzystania licencji
c) Raport wykonanych zadań backupowych
d) Raporty obciążenia serwerów backupowych – minimum monitorowanie użycia CPU i pamięci RAM.

6.94. System musi mieć możliwość automatycznego wysyłania dowolnych raportów do wybranych użytkowników poprzez mail.

6.95. System musi mieć możliwość automatycznego zapisywania raportów w formacie minimum: PDF, HTML i CSV.

6.96. Notyfikacje alertów muszą być wysyłane minimum poprzez mail.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

6.97. System musi zapewniać funkcjonalność wznawiania zadań backupowych.

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

6.99. System musi zapewniać funkcjonalność wykonywania zadania backupu wieloma równoległymi strumieniami – tzw. multistreaming. Polega ona na tym, iż 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

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

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

6.102. System musi posiadać możliwość wykonywania backupu pełnego, przyrostowego, różnicowego oraz syntetycznego.

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

6.104. System ma realizować procesy backupu oraz odzyskiwania danych, procesy te muszą być uruchamiane ręcznie i poprzez wbudowany kalendarz, możliwość definiowania zadań poprzez wbudowany w system kalendarz musi być możliwa nie tylko dla zadań backupowych, ale także dla zadań odtwarzania danych, a więc restore.

6.105. System musi posiadać (jako opcja) zintegrowane w systemie mechanizmy indeksowania pełnokontekstowego i wyszukiwania danych. Indeksowaniu powinny podlegać dane zbackupowane i zarchiwizowane już znajdujące się w systemie.

6.106. System musi realizować funkcjonalność weryfikacji wykonanych kopii.

6.107. System powinien umożliwiać składowanie kopii backupowych na storage obiektowym w chmurze, minimum: Azure, Amazon, Google Cloud, jeśli do włączenia tej funkcjonalności potrzebne są jakieś dodatkowe komponenty to muszą być zaoferowane.

6.108. Możliwość zwiększenia bezpieczeństwa systemu poprzez integrację z CyberArk pozwalająca na przechowywanie kont i haseł także dla aplikacji w środowisku CyberArk a nie w środowisku backupowych. Integracja musi pozwalać na rotacyjną zmianę haseł i ich synchronizację w środowisku.

6.109. Musi istnieć możliwość wskazania klucza szyfrującego (Bring Your Own Key – BYOK), który będzie wykorzystywany do szyfrowania kopii backupowych.

6.110. Automatyzacja – zarządzanie systemem poprzez API, Terraform, Ansible i PowerShell.

6.111. Workflow – dedykowany komponent do tworzenia i uruchamiania procesów obejmujących działania w obszarze backupu, odtwarzania oraz pozwalający na wykonywanie poleceń czy skryptów z systemów zewnętrznych.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

6.112. Podstawowe komponenty systemu jak: serwer zarządzający, serwery składujące i deduplikujące dane muszą wspierać system operacyjny Linux, a więc musi istnieć możliwość bezpośredniego zainstalowania na systemie Linux tych komponentów bez jakiejkolwiek warstwy wirtualizacyjnej.

6.113. System musi oferować integrację z mechanizmami deduplikacyjnymi urządzeń typu appldeduplikator minimalne wsparcie to DDBoost i Catalyst (urządzenia: Dell Data Domain, HPE StoreOnce). Integracja z deduplikatorami musi być dostępna nie tylko dla Windows, ale także dla Linux i wspierać tzw. client direct (transfer danych bezpośrednio na urządzenia deduplikacyjne a tylko metadane wysyłane do systemu backupowego

7. Wymagania jakościowe i organizacyjne (SLA)

Usługi wsparcia będą świadczone zgodnie z parametrami jakościowymi:

7.1. Kontakt z działem wsparcia technicznego producenta w celu uzyskania pomocy technicznej dotyczącej oprogramowania za pośrednictwem poczty elektronicznej, poprzez stronę www, telefonicznie w dni od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy oraz dni wolnych u Zamawiającego, w godzinach od 8:00 do 16:00.

7.2. Pomoc techniczna mająca na celu rozwiązywanie powtarzalnych i możliwych do rozwiązania problemów związanych z oprogramowaniem. Udzielanie wsparcia przy identyfikacji problemów trudnych do powtórzenia. Wsparcie przy rozwiązywaniu problemów, pomoc w określaniu parametrów konfiguracji oprogramowania oraz wstępne obejścia wykrytych problemów. Pomoc techniczna będzie udzielana zdalnie za pośrednictwem poczty elektronicznej.

7.3. Dostęp do dokumentacji technicznej oprogramowania, w tym do najnowszych wersji dokumentów oraz oprogramowania. Dostęp do dokumentacji będzie udzielany poprzez stronę internetową (portal producenta).

7.4. Dostęp do aktualizacji oraz poprawek oprogramowania. Dostęp do aktualizacji będzie udzielany poprzez stronę internetową (portal producenta).

Osoba/y sporządzająca Grzegorz Magryta

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706