(164936)

**Opis przedmiotu Zamówienia (OPZ)**

1. **Przedmiotem zamówienia** jest: **„Rozbudowa systemu backupu w Centrum e-Zdrowia – Cyfrowy Bunkier."**

2. Zamawiający użytkuje na potrzeby DataCenter system zabezpieczenia danych stworzony w oparciu o:
   - aplikacje backup'owe
     - Commvault
     - Veeam Backup and Replication
   - urządzenia do składowania danych backup'owych
     - 4x deduplikator PowerProtect DataDomain 9400 (dalej w dokumencie DD).
     - 2x deduplikator PowerProtect DataDomain 9300(dalej w dokumencie DD).

3. Rozbudowa w/w środowiska o część: Cyfrowy Bunkier (zwanym dalej „CB") obejmuje:
   - Dostawę kompletnego systemu informatycznego zapewniającego odtworzenie po ataku typu ransomware, tj.: deduplikator wraz z niezbędną infrastrukturą serwerowo-sieciowo-aplikacyjną, oprogramowaniem i licencjami szczegółowo opisanymi w pkt.3.1 oraz pkt.3.2 i 3.3;
   - Wdrożenie rozwiązania;
   - Świadczenie gwarancji i usług wsparcia serwisowego przez okres 60 miesięcy;
   - Świadczenie usług wsparcia eksperckiego;
   - Wykonanie dokumentacji powykonawczej;
   - Przeprowadzenie instruktażu.

3.1. **Wymagania Ogólne:**

Podstawowe ogólne funkcjonalności:

- Utworzenie trzeciej warstwy danych backup'owych w oparciu o dane już składowane na eksploatowanych urządzeniach Data Domain (DD), wymagane dodatkowe medium dedykowane do przechowywania tych danych wraz z niezbędną infrastrukturą serwerowo-sieciowo-aplikacyjną,
- zapewnienie niezmienności przechowywanych danych w okresie zaplanowanej retencji,
- wprowadzenie analityki wybranych danych z CB, pod kątem zainfekowania przez ransomware,
- wprowadzenie mechanizmu raportującego umożliwiającego wskazanie danych zainfekowanych oraz danych niezainfekowanych mogących posłużyć za źródło odtwarzania systemów.

3.1.1. Całkowita integracja oferowanego CB z aktualnie eksploatowanym środowiskiem zabezpieczania danych w tym:



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

- bezpośrednia synchronizacja danych pomiędzy aktualnie eksploatowanymi przez Zamawiającego urządzeniami DD oraz urządzeniem dedykowanym do przechowywania trzeciej kopii danych w CB w oparciu o mechanizm MTree replication,
- automatyzm w/w synchronizacji danych zgodnie z wprowadzonymi politykami zarówno w przypadku planu synchronizacji, okna synchronizacji, objęcia przesłanych danych blokadą zapewniającą niezmienność danych,
- możliwość przeprowadzania stałej, cyklicznej, pełnej („full content") i bezpośredniej (bez pośrednictwa serwerów zarządzających) analizy danych zapisanych pod kątem zainfekowania przez ransomware,
- możliwość przeprowadzenia „odwrotnej" bezpośredniej synchronizacji wybranych danych do środowiska produkcyjnego.

3.1.2. Niezbędnym elementem jest dostosowanie danych składowanych na obecnie eksploatowanych urządzeń DD, mające na celu możliwość implementacji rozwiązania CB. Polegać będzie ono na wydzieleniu wskazanych przez Zamawiającego kluczowych danych podlegających replikacji do CB, umożliwiającym zainicjowanie całego procesu, co może wiązać się z koniecznością przeorganizowania danych składowanych na urządzeniach DD , oraz koniecznością wprowadzenia dodatkowej struktury katalogowej przechowującej wskazane dane.

3.1.3. Zastosowany mechanizm umożliwiający analitykę składowanych w CB danych musi:

- umożliwiać jednoczesną analizę całej zawartości składowanych danych zarówno „full content" oraz analizę ich metadanych,
- wykrywać infekcję typu ransomware zarówno w oparciu o metody statystyczne oraz algorytmy samouczące,
- obsługiwać metody analizy obejmujące aktualnie rozpoznane metody ataku ransomware co najmniej:
  - silne szyfrowanie z oryginalną nazwą pliku,
  - częściowe silne szyfrowanie z oryginalną nazwą pliku,
  - silne szyfrowanie RMS/MS_EFS,
  - silne szyfrowanie z nowym znanym rozszerzeniem,
  - częściowe silne szyfrowanie z nowym znanym rozszerzeniem,
  - silne szyfrowanie z zaciemnioną nazwą pliku,
  - szyfrowanie strony bazy danych,
  - nowe rozszerzenie pliku,
  - ukrycie nazwy pliku,
  - słabe szyfrowanie z nowym rozszerzeniem pliku,
  - słabe szyfrowanie z oryginalną nazwą pliku,
  - częściowe szyfrowanie z zaciemnioną nazwą pliku,
  - szyfrowanie wewnątrz z oryginalną nazwą pliku,
  - częściowo słabe szyfrowanie z oryginalną nazwą pliku i typem pliku,
  - słabe szyfrowanie z zaciemnioną nazwą pliku,
  - archiwum grupowe utrzymujące wymazaną oryginalną nazwę pliku,
  - silne szyfrowanie z nowym znanym rozszerzeniem — usuwanie zduplikowanych plików,



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

- wypełnienie zerami z nowym znanym rozszerzeniem,
- wypełnienie zerami z oryginalną nazwą pliku,
- wypełnienie zerami z zaciemnioną nazwą pliku.

- posiadać wsparcie dla baz Oracle, Microsoft SQL Server, Mongo DB.

3.1.4. **Termin rozbudowy systemu backupu – maksymalnie 90 dni kalendarzowych** od dnia zawarcia Umowy, na warunkach określonych w punkcie 6.

3.1.5. CB musi być rozwiązaniem kompletnym, appliancem sprzętowym pochodzącym od jednego producenta. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway. Oferowany typ urządzenia musi być oficjalnie dostępny w ofercie producenta i znajdować się w sprzedaży od co najmniej 60 dni poprzedzających termin otwarcia ofert.

3.1.6. Wymagane 60-cio miesięczna gwarancja i wsparcie serwisowe działające w trybie 24x7 od dnia podpisania Protokołu odbioru, umożliwiające upgrade oprogramowania sprzętowego do najnowszej wersji. W ramach wymaganego wsparcia uszkodzone nośniki danych (dyski twarde) pozostają u Zamawiającego bez ponoszenia dodatkowych kosztów.

3.2. **Wymagania szczegółowe dotyczące Cyfrowego Bunkra:**

| L.p. | Treść wymagania |
|---|---|
| 1. | Cyfrowy Bunkier – kompletny system informatyczny zapewniający odtworzenie po ataku typu ransomware musi zawierać:<br><br>a) **Deduplikator** do przechowywania backupów produkcyjnych – szczegółowe wymagania przedstawione w dalszej części dokumentu,<br>b) Infrastrukturę aplikacyjno-serwerową (nazwana na potrzeby OPZ- **I1**) umożliwiającą zarządzanie automatyczną bezpośrednią synchronizacją danych a także ustawianiem ich w trybie Compliance, pomiędzy aktualnie eksploatowanymi urządzeniami DD oraz Deduplikatorem będącym przedmiotem zamówienia,<br>c) Infrastrukturę aplikacyjno-serwerową (nazwana na potrzeby OPZ **I2**) umożliwiającą przeprowadzanie cyklicznej (każdego dnia) analityki przechowywanych danych na Deduplikatorze, a także raportowanie,<br>d) Infrastrukturę sieciową (**NET**) umożliwiającą połączenie dostarczonych elementów, zapewniającą odpowiednią ilość portów oraz przepustowość (w zależności od dostarczanego rozwiązania).<br><br>CB musi składać się z elementów pochodzących od jednego producenta, oznaczonych nazwą i numerem katalogowym producenta, dostępnych na dzień-złożenia oferty.<br><br>Oferowane rozwiązanie CB musi zostać opatrzone wszelkimi niezbędnymi usługami wdrożeniowo-implementacyjnymi niezbędnymi do uruchomienia produkcyjnego oferowanego środowiska. |



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

| | |
|---|---|
| 2. | Dostarczone rozwiązanie CB musi składać się z urządzeń fabrycznie nowych, nieużywanych, wyprodukowanych nie wcześniej niż 6 miesięcy przed datą otwarcia oferty, wolnych od wad fizycznych i prawnych.<br><br>Oferowane urządzenia i oprogramowanie nie mogą być prototypem co oznacza, że identyczne modele urządzeń oraz wersje oprogramowania muszą znajdować się w sprzedaży, od co najmniej 60 dni poprzedzających termin otwarcia ofert. |
| 3. | CB musi umożliwiać replikację oraz przechowywanie całości backupów produkcyjnych pochodzących z aplikacji Commvault/Veeam, składowanych aktualnie na urządzeniach DD. |
| 4. | CB musi mieć możliwość przechowania na oferowanym Deduplikatorze minimum 0,4 PB danych produkcyjnych (źródłowych) z retencją co najmniej 30 dni przy założeniu codziennej synchronizacji danych. |
| 5. | CB musi posiadać Deduplikator, który swoje wymagania ma opisane punkcie 3.3. Wymagania szczegółowe dotyczące Deduplikatora. |
| 6. | CB musi być odizolowany od środowiska produkcyjnego co m.in. oznacza:<br><br>a) Deduplikator wchodzący w skład CB nie może znajdować się w DNS / AD, nie jest używany jego FQDN,<br>b) w systemach po stronie produkcyjnej nie może być używany adres IP Deduplikatora wchodzącego w skład CB (wymaganie dotyczy również aplikacji backupowych),<br>c) wykluczona jest możliwość komunikacji ze strony produkcyjnej w przypadku użycia: ping, https, http, ssh czy innych standardowych metod z Deduplikatorem wchodzącym w skład CB,<br>d) możliwość komunikacji między eksploatowanym urządzeniem DD, a Deduplikatorem wchodzącym w skład CB musi odbywać się wyłącznie poprzez protokół replikacyjny. |
| 7. | CB musi obejmować infrastrukturę **I1** automatyzującą synchronizację backupów produkcyjnych do CB. Mechanizm automatyzacji synchronizacji danych do CB musi umożliwiać m.in.:<br><br>a) definicję kalendarza synchronizacji danych do CB, wymagana częstotliwość synchronizacji w przedziale 1h do 24h z gradacją wynoszącą min. 1h,<br>b) automatyczne wyłączanie portu komunikacyjnego między Deduplikatorem będącym częścią składową CB a eksploatowanym DD (poza okresem synchronizacji danych),<br>c) tworzenie do 500 snapshotów wybranego zrzutu na Deduplikatorze będącym częścią składową CB,<br>d) ręczną inicjalizację blokady (Compliance) na wybranych snapshotach,<br>e) automatyczną inicjalizację blokady na snapshotach zrzutów (Compliance),<br>f) podłączanie snapshotów do serwerów w CB poprzez protokół nfs (sandbox). |



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

| | |
|---|---|
| 8. | CB musi obejmować Infrastrukturę **I2** umożliwiającą analizę zreplikowanych danych pod kątem ataku ransomware, wymagane funkcjonalności:<br><br>a) definicja kalendarza skanowania zreplikowanych danych musi być możliwa z poziomu centralnego oprogramowania CB,<br>b) skanowaniu/analizie pod kątem ataku ransomware muszą podlegać:<br><br>• metadane plików<br>• zawartość plików (full-content)<br><br>c) etap skanowania musi obejmować serię analiz plików oraz baz danych, zastosowany mechanizm musi rozpoznawać format plików oraz baz danych, a także weryfikować ich poprawność pod kątem ataku ransomware,<br>d) możliwość analizy/skanowania zawartości backupów obejmujących zasoby maszyn wirtualnych VMware pod kątem ataku ransomware,<br>e) efekty działania systemu realizującego analizę danych muszą być logowane (zapisywane do tzw. Event Log),<br>f) w celu optymalizacji wydajności, mechanizm skanowania powinien wykrywać dane które zmieniły się w stosunku do ich ostatnio analizowanej kopii oraz przeprowadzać analizę części zmienionych/nowych,<br>g) wymagane licencje umożliwiające ciągłą analizę kopii danych będących efektem działania aplikacji backupowych na wolumenie0,2 PB FET,<br>h) wyskalowanie infrastruktury I2 musi umożliwiać analizę w trybie dziennym, zreplikowanych danych będących efektem działania aplikacji backupowych na wolumenie 0,2 PB FET. |
| 9. | Zakres wymaganych usług:<br><br>a) instalacja wszystkich elementów wchodzących w skład proponowanego rozwiązania,<br>b) implementacja CB zgodnie z przedstawionymi wymaganiami ogólnymi i szczegółowymi,<br>c) implementacja mechanizmu synchronizacji danych produkcyjnych z CB,<br>d) implementacja systemu umożliwiającego analizę synchronizowanych danych pod katem ataku ransomware,<br>e) implementacja wydzielonych środowisk systemu backupowego Commvault/Veeam w CB umożliwiających zarządzanie synchronizowanymi kopiami. |

3.3. **Wymagania szczegółowe dotyczące Deduplikatora wchodzącego w skład CB:**

| L.p. | Treść wymagania |
|---|---|



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

| | |
|---|---|
| 1. | Urządzenie musi być przeznaczone do deduplikacji i przechowywania kopii zapasowych. |
| 2. | Urządzenie musi oferować pojemność minimum 1,45 PB netto (nie wliczając nadmiarowości potrzebnej do zabezpieczenia danych np.: RAID) - dedykowanej do przechowywania deduplikatów przestrzeni użytkowej. Oferowana pojemność netto nie może zawierać w sobie przestrzeni typu cloud. |
| 3. | Oferowane urządzenie musi posiadać minimum (ilość i przepustowość):<br>• 4 porty Eth 100 Gb/s OP (wymagana pełna obsada wkładek)<br>• 8 portów Eth 10/25 Gb/s OP (wymagana pełna obsada wkładek)<br>• 4 porty FC 16Gb/s OP (wymagana pełna obsada wkładek) |
| 4. | Oferowane urządzenie musi umożliwiać jednoczesny dostęp wszystkimi poniższymi protokołami:<br>• CIFS, NFS,<br>• zapewniającymi deduplikację na źródle, wymagane wsparcie dla używanych przez Zamawiającego wyspecyfikowanych w wymaganiach aplikacji backupowych. |
| 5. | O ile to niezbędne, wymagane jest dostarczenie licencji, pozwalającej na jednoczesną obsługę protokołów CIFS, NFS, deduplikacja na źródle. |
| 6. | Oferowane pojedyncze urządzenie musi osiągać zagregowaną wydajność (dla maksymalnej konfiguracji) protokołami: **NFS** co najmniej 50 TB/h (dane podawane przez producenta) oraz co najmniej 100 TB/h z wykorzystaniem **deduplikacji na źródle** (dane podawane przez producenta). |
| 7. | Urządzenie musi pozwalać na jednoczesną obsługę minimum 1800 strumieni w tym jednocześnie: zapis danych minimum 500 strumieniami.<br>• odczyt danych minimum 300 strumieniami,<br>• replikacja (jako urządzenie docelowe) minimum 1000 strumieniami, pochodzących z różnych aplikacji oraz dowolnych protokołów (CIFS, NFS, deduplikacja na źródle) oraz dowolnych interfejsów (FC, LAN) w tym samym czasie.<br>Wymieniona wartość 1800 jednoczesnych strumieni dla wszystkich protokołów musi mieścić w przedziale oficjalnie rekomendowanym i wspieranym przez producenta urządzenia.<br><br>Wszystkie zapisywane strumienie muszą podlegać globalnej deduplikacji przed zapisem na dysk (in-line). |
| 8. | Oferowane urządzenie musi deduplikować dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia. |
| 9. | Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku jednak o długości nie większej niż 12 kB. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych co oznacza, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości, bez konieczności podejmowania czynności mających na celu ustalenie predefiniowanej długości bloków używanych do deduplikacji |



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

| | |
|---|---|
| | danych określonego typu. Deduplikacja zmiennym, dynamicznym blokiem oznacza, że wielkość każdego bloku (na jaki są dzielone dane pojedynczego strumienia backupowego) może być inna niż poprzedniego oraz jest indywidualnie ustalana przez algorytm deduplikacji zastosowany w urządzeniu, oferowane urządzenie nie może dzielić jakiegokolwiek pojedynczego strumienia danych backupowych na bloki o ustalonej, tej samej długości. |
| 10. | Oferowany produkt musi posiadać obsługę mechanizmów globalnej deduplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, VTL, deduplikacja na źródle) przechowywanych w obrębie całego urządzenia co oznacza, że przechowywany na urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany. Wszystkie udziały NFS/CIFS również powinny podlegać globalnej deduplikacji – blok danych otrzymany i zapisany w wirtualnej bibliotece „A", nie może zostać ponownie zapisany, jeśli trafi do innej wirtualnej biblioteki „B" w obrębie tego samego urządzenia (to samo dotyczy udziałów NFS/CIFS). Przestrzeń składowania zdeduplikowanych danych musi być jedna dla wszystkich protokołów dostępowych, co oznacza zastosowanie pojedynczej bazy deduplikatów bez względu na ilość/rodzaj używanych jednocześnie protokołów dostępowych. |
| 11. | Zapisowi na system dyskowy mogą podlegać tylko unikalne bloki danych nie zapisane jeszcze na system dyskowy urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych. |
| 12. | Oferowane rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej) w celu ich późniejszej deduplikacji (wymagana deduplikacja in-line). |
| 13. | Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo kompresowane. |
| 14. | Tryb zapisu zabezpieczanych danych nie powinien umożliwiać nadpisywania danych, dane mogą być zapisywane jedynie w trybie append-only. Dane dla których wygasła retencja powinny zostać usunięte podczas procesu czyszczenia tzw. cleaning. |
| 15. | Oferowane urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia), wyspecyfikowane wcześniej aplikacje backupowe eksploatowane przez Zamawiającego w trybie zapisu deduplikacji na źródle. |
| 16. | Oferowane urządzenie powinno umożliwiać uruchamianie maszyn wirtualnych VMware bezpośrednio z danych backupowych bez konieczności odtwarzania danych, . |
| 17. | W przypadku deduplikacji na źródle poprzez sieć IP (LAN oraz WAN), wymagana jest możliwość szyfrowania komunikacji kluczem minimum 256 bitów. |
| 18. | Urządzenie powinno umożliwiać zaszyfrowanie przechowywanych danych. Wykonawca dostarczy wymagane licencje umożliwiające zaszyfrowanie i przechowywanie zaszyfrowanych danych w obrębie maksymalnej pojemności oferowanego urządzenia, jeśli takie licencje będą wymagane. |
| 19. | Deduplikator wchodzący w skład CB musi umożliwiać zestawienie równoległej jednoczesnej replikacji wielu niezależnych zasobów danych, znajdujących się na urządzeniach DD Zamawiającego, będących efektem działania zarówno wymienionych wcześniej aplikacji backupowych jak i będących efektem backupu wbudowanymi narzędziami bazodanowymi (RMAN, Microsoft SQL Server |



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

| | |
|---|---|
| | Management Studio). W przypadku danych replikacyjnych różnych zasobów, wymagana jest możliwość:<br><br>a) zmiany retencji w stosunku do backupów źródłowych,<br>b) niezależnego równoległego odtwarzania,<br>c) założenia wymaganej blokady zapewniającej Compliance. |
| 20. | Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych z aktualnie eksploatowanymi przez Zamawiającego urządzeniami DD. Konfiguracja replikacji musi być możliwa w każdym z trybów:<br><br>• jeden do jednego<br>• wiele do jednego<br>• jeden do wielu<br>• kaskadowej (urządzenie A replikuje dane do urządzenia B, które te same dane replikuje do urządzenia C) Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu. Wykonawca dostarczy wymagane licencje na replikację, jeśli takie licencje będą wymagane. Replikacja musi wspierać dane objęte blokadą (na eksploatowanych urządzeniach DD) we wszystkich dostępnych trybach. Dane zreplikowane muszą automatycznie być objęte taką samą blokadą jak na urządzeniu źródłowym. |
| 21. | Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych do replikacji, spośród puli portów określonych w punkcie 3.3 wymagań szczegółowych dot. Deduplikatora. |
| 22. | W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami. |
| 23. | W przypadku replikacji danych między dwoma urządzeniami oferowanego typu, wymagana możliwość kontroli przez Commvault.<br><br>Wymagane są następujące funkcjonalności:<br><br>• replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących,<br>• replikacji podlegają tylko te fragmenty danych, które nie znajdują się na docelowym urządzeniu,<br>• replikacja zarządzana jest z poziomu wymaganej aplikacji,<br>• aplikacja posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach bez konieczności przeprowadzania procesu inwentaryzacji. |
| 24. | Oferowane urządzenie musi działać poprawnie przy zapełnieniu danymi na poziomie co najmniej 90%. Dokumentacja urządzenia nie może wskazywać na ewentualne problemy, obostrzenia, które są efektem zapełnienia urządzenia zabezpieczanymi danymi, na poziomie mniejszym niż 90%. |



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

| | |
|---|---|
| 25. | Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami – oferowane urządzenie powinno być wyposażone w mechanizm umożliwiający zarządzanie stopniem wykorzystania pasma na potrzeby replikacji. |
| 26. | Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6. |
| 27. | Każda grupa RAID 6 musi mieć przynajmniej 1 dysk hot-spare automatycznie włączany do grupy RAID w przypadku awarii jednego z dysków produkcyjnych. Dyski hot-spare muszą być globalne, możliwe do wykorzystania w innych (pozostałych) grupach RAID. |
| 28. | Oferowane urządzenie musi umożliwiać wykonywanie snapshot-ów, czyli umożliwiać zamrożenie obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane urządzenie musi również umożliwiać odtworzenie danych ze snapshot-a. Odtworzenie danych ze snapshot-u nie może wymagać konieczności nadpisania danych produkcyjnych jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania/ odtwarzania backupów). Wymagana możliwość wykorzystania funkcjonalności snapshot dla danych przesyłanych dowolnym z wymaganych interfejsów urządzenia. |
| 29. | Urządzenie musi pozwalać na przechowywanie minimum 700 snapshot-ów jednocześnie w obrębie oferowanej przestrzeni, przy zachowaniu globalnej deduplikacji oraz standardowego trybu pracy urządzenia – umożliwiającego wykorzystanie wszystkich dostępnych funkcjonalności. |
| 30. | Urządzenie musi umożliwiać podział na logiczne części. Dane znajdujące się w każdej logicznej części muszą być między sobą deduplikowane (globalna deduplikacja między logicznymi częściami urządzenia). |
| 31. | Urządzenie musi mieć możliwość podziału na minimum 20 logicznych części pracujących równolegle. Producent musi oficjalnie wspierać pracę minimum 20 logicznych części pracujących równolegle z pełną wydajnością urządzenia. |
| 32. | Dla każdej z w/w logicznych części oferowanego urządzenia musi być możliwość zdefiniowania oddzielnego użytkownika zarządzającego daną logiczną częścią deduplikatora. Użytkownicy zarządzający logiczną częścią A muszą widzieć tylko i wyłącznie zasoby logicznej części A i nie mogą widzieć żadnych innych zasobów oferowanego urządzenia. |
| 33. | Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia, jako niezależnego urządzenia dostępnego za pośrednictwem:<br>• CIFS<br>• NFS<br>• Deduplikacja na źródle |
| 34. | Urządzenie powinno umożliwiać zdefiniowanie blokady skasowania danych (funkcjonalność WORM). Blokada skasowania danych musi chronić plik w zdefiniowanym czasie przed usunięciem pliku oraz modyfikacją pliku. |



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

| | |
|---|---|
| | Blokada skasowania danych musi działać w dwóch trybach (do wyboru przez administratora):<br>1. możliwość zdjęcia blokady przed upływem ważności danych (retencją),<br>2. brak możliwości zdjęcia blokady przed upływem ważności danych (COMPLIANCE) wymagane oficjalne wsparcie wymaganej blokady przez aplikację Commvault, oraz Veeam Backup and Replication– wymagane potwierdzenie na oficjalnych stronach w/w aplikacji backup'owych oraz producenta oferowanego deduplikatora<br>3. Wymagana blokada (COMPLIANCE) ze względów bezpieczeństwa musi posiadać mechanizm wewnętrznego zegara, aby zapobiec skutkom potencjalnej złośliwej ingerencji w zegar systemowy, blokada musi wyeliminować możliwość zmiany aktualnej daty oraz czasu.<br>Wymagana blokada (COMPLIANCE) musi blokować możliwość systemowego zniszczenia systemu plików.<br><br>Wymagana blokada w oferowanym Deduplikatorze, musi spełniać najsurowsze wymagania dotyczące trwałości danych, określone następującymi przepisami:<br><br>a) SEC 17a-4(f)<br>b) CFTC Rule 1.31b<br>c) FDA 21 CFR Part 11<br>d) Sarbanes-Oxley Act<br>e) IRS 98025 and 97-22<br>f) ISO Standard 15489-1<br>g) MoREQ2010<br><br>Wymagana funkcjonalność replikacji oraz blokady WORM muszą oficjalnie wspierać możliwość replikacji danych objętych blokadą z aktualnie eksploatowanych przez Zamawiającego deduplikatorów DD, proces replikacji powinien zakończyć się zainicjalizowaniem blokady danych zreplikowanych w takim trybie jaki był użyty w przypadku danych oryginalnych. O ile to niezbędne, licencje na blokadę usunięcia/zmiany przechowywanych plików muszą być dostarczone wraz z urządzeniem. |
| 35. | Urządzenie musi weryfikować dane po zapisie (nie chodzi o ew. weryfikację danych indeksowych generowanych przez urządzenie, ale o weryfikację wszystkich zabezpieczanych danych backup'owych). Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie. Powyższa weryfikacja powinna być realizowana w locie, czyli przed usunięciem z pamięci oryginalnych danych (otrzymanych z aplikacji backupowej), musi być realizowana w trybie ciągłym (a nie ad-hoc), wymagane parametry wydajnościowe urządzenia muszą uwzględniać tę funkcjonalność.<br><br>Wymagane potwierdzenie opisanej funkcjonalności w oficjalnej dokumentacji producenta oferowanego urządzenia. |



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

| | |
|---|---|
| 36. | Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia. |
| 37. | Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu). |
| 38. | Wymagana jest możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora). |
| 39. | Wymagana jest możliwość zdefiniowania harmonogramu wg. którego wykonywany jest proces usuwania przeterminowanych danych (czyszczenia), realizowany równolegle z procesami backup/restore/replication. |
| 40. | Standardowa częstotliwość usuwania przeterminowanych danych (czyszczenie) nie powinna być większa niż 1 raz na tydzień - minimalizując czas, w którym backupy/odtworzenia narażone są na spowolnieni. |
| 41. | Urządzenie musi mieć możliwość zarządzania poprzez:<br>• Interfejs graficzny dostępny z przeglądarki internetowej<br>• Poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell) |

**4.** Zasady świadczenia usługi gwarancji i wsparcia serwisowego sprzętu i oprogramowania:

4.1. Wykonawca od dnia podpisania Protokołu odbioru świadczył będzie usługę gwarancji i wsparcia przez okres 60 miesięcy.

4.2. Wykonawca w odniesieniu do usług gwarancji i wsparcia serwisowego zapewni całodobowe przyjmowanie zgłoszeń przez 7 dni w tygodniu, przez 365/366 dni w roku. Zgłoszenia powinny być przyjmowane za pomocą portalu serwisowego, numeru telefonu lub na adres poczty elektronicznej podany przez Wykonawcę.

4.3. Wykonawca zobowiązuje się nie później niż w ciągu 1 dnia roboczego od momentu otrzymania zgłoszenia awarii potwierdzić przyjęcie zgłoszenia.

4.4. Wykonawca rozwiąże zgłoszone problemy, a w przypadku braku możliwości usunięcia awarii zastosuje rozwiązanie tymczasowe i przywróci pełną sprawność CB w ciągu 2 dni roboczych od momentu zgłoszenia przez Zamawiającego.

4.5. W przypadku, gdy naprawa nie może być wykonana w terminie 2 dni roboczych od momentu zgłoszenia, Wykonawca dostarczy, uruchomi i skonfiguruje sprzęt zastępczy, w terminie 4 dni roboczych, wyprodukowany nie wcześniej niż wymieniany, wykonany w tej samej technologii, o nie gorszych parametrach technicznych i o nie większych kosztach eksploatacji, przez cały okres użytkowania sprzętu przez Zamawiającego. Sprzęt zastępczy musi być zgodny programowo z urządzeniem uszkodzonym (tzn. umożliwiać osadzenia na nim identycznego oprogramowania) i posiadać wszelkie niezbędne licencje. Sprzęt zastępczy nie będzie powodował wzrostu kosztów utrzymania pozostałych urządzeń posiadanych przez Zamawiającego. Koszty dostawy i wymiany sprzętu ponosi Wykonawca. Sprzęt zastępczy będzie uruchomiony na okres nie dłuższy niż 60 dni. Po tym terminie Wykonawca jest zobowiązany do dostarczenia naprawionego sprzętu. W przypadku, gdy Wykonawca nie zwróci naprawianego sprzętu w powyższym terminie lub Umowa wygaśnie przed



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

upływem 60 dni od dostarczenia sprzętu zastępczego sprzęt zastępczy przechodzi na własność Zamawiającego, co zostanie potwierdzone podpisaniem przez Strony protokołu. Podstawiony sprzęt zastępczy będzie objęty identycznymi warunkami usługi gwarancji i wsparcia serwisowego, jak dla sprzętu będącego w posiadaniu Zamawiającego.

4.6. Części wymontowane ze sprzętu (z wyjątkiem dysków twardych) stają się własnością Wykonawcy, natomiast części dostarczone przez Wykonawcę z chwilą ich wymiany przechodzą na własność Zamawiającego. W przypadku wymiany dysków twardych, zarówno uszkodzony jak i nowo dostarczony dysk, pozostają własnością Zamawiającego. Części zamontowane w sprzęcie przez Wykonawcę, będą wyprodukowane nie wcześniej niż wymieniane, wykonane w tej samej technologii, o nie gorszych parametrach technicznych i o nie większych kosztach eksploatacji, przez cały okres użytkowania sprzętu przez Zamawiającego. Części zamontowane w sprzęcie przez Wykonawcę, nie będą powodowały wzrostu kosztów utrzymania urządzenia, w którym część została zamontowana oraz kosztów utrzymania pozostałych urządzeń posiadanych przez Zamawiającego. Koszty dostawy i wymiany części ponosi Wykonawca;

4.7. W przypadku awarii nośnika danych (dysk twardy) Zamawiający zatrzymuje uszkodzony nośnik i wymaga od Wykonawcy dostarczenia nowego nośnika i wymiany uszkodzonego na nowy. Dostarczony, nowy nośnik nie może mieć gorszych parametrów niż wymieniany nośnik uszkodzony. W przypadku wymiany dysków twardych, również w ramach gwarancji lub rękojmi, zarówno uszkodzony jak i nowo dostarczony dysk, pozostają własnością Zamawiającego.

4.8. W przypadku, jeżeli producent oprogramowania wbudowanego udostępni jakiekolwiek aktualizacje, nowe wersje, patche, zmiany itp. (dalej łącznie zwane aktualizacjami), Wykonawca w ramach usługi gwarancji i wsparcia serwisowego zapewni Zamawiającemu dostęp do tych aktualizacji oraz przekaże prawa do użytkowania aktualizacji oprogramowania, niezwłocznie po ich udostępnieniu poprzez jedną z dróg: stronę www, pendrive.

4.9. Wykonawca dokona instalacji aktualizacji i nowych wersji oprogramowania wbudowanego, w terminach uzgodnionych z Zamawiającym. Decyzja o wykonaniu aktualizacji oprogramowania należy wyłącznie do Zamawiającego, a Wykonawca nie jest uprawniony do zgłaszania wobec Zamawiającego żądania instalacji danej aktualizacji. Wykonawca może uprzedzić Zamawiającego o konsekwencjach niedokonania aktualizacji.

4.10. Usługa gwarancji i wsparcia serwisowego sprzętu będzie świadczona w języku polskim.

4.11. Usługa gwarancji i wsparcia serwisowego będzie świadczona na terenie Polski.

**5. Wykonawca zapewni również wsparcie eksperckie**

5.1. Wykonawca ma obowiązek udzielenia konsultacji dla Zamawiającego w wymiarze **100 godzin eksperckich**, w terminach wcześniej uzgodnionych pomiędzy stronami. Zamawiający zakłada, że konsultacje obejmujące przedmiot zamówienia będą realizowane zdalnie. Zamawiający dopuszcza jednak zlecenie określonych prac w siedzibie Zamawiającego.

**6.** Sposób rozbudowy

6.1. Rozbudowa systemu do backupu zostanie zrealizowana w terminie do 90 dni kalendarzowych od dnia zawarcia Umowy.



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

6.2. Wszystkie czynności Wykonawcy składające się na rozbudowę muszą uwzględniać charakterystykę systemu backupu Zamawiającego, w tym obecnie eksploatowane urządzenia.

6.3. Rozbudowa systemu backup składa się z następujących etapów:

6.3.1. Rozbudowa właściwa

Wykonawca zobowiązany jest do:

a) Zaplanowania konfiguracji połączeń, przy współpracy z administratorami Zamawiającego, z uwzględnieniem konfiguracji finalnej
b) Dostarczenie sprzętu do lokalizacji wskazanej przez Zamawiającego wraz z niezbędnymi akcesoriami koniecznymi do ich montażu i uruchomiania takie jak: śrubki, nakrętki, okablowanie itp.
c) Rozpakowania, montaż, uruchomienie, konfiguracji, testów diagnostycznych dostarczonego sprzętu wraz z niezbędnym oprogramowaniem,
d) Wdrożenia CB do systemu backupu.

6.3.2. Odbiór rozbudowy:

6.3.2.1. Zamawiający i Wykonawca przystąpią do weryfikacji prawidłowości dokonanej rozbudowy

6.3.2.2. Warunkiem odbioru rozbudowy będzie spełnienie przez Wykonawcę kryteriów odbioru.

6.3.2.3. Kryteriami odbioru są:

6.3.2.3.1. Podpisane obustronnie bez uwag Protokołu odbioru:

a) Szczegółowa dokumentacja powykonawcza, uwzględniająca:

- Protokół odbioru dostarczonych urządzeń,
- Protokół instalacji i testów diagnostycznych,
- Konfigurację dostarczonych urządzeń,
- Schematy urządzeń oraz połączeń między nimi.

b) Rutynowe Procedury Operatora i Administratora dotyczące:

- Monitorowania wydajności urządzeń za pomocą oprogramowania dostarczonego w ramach zamówienia.
- Wyświetlenia konfiguracji urządzeń za pomocą oprogramowania dostarczonego w ramach zamówienia.

**7.** W ramach Rozbudowy, Wykonawca zobowiązany jest do:

7.1. Koordynowania prac;

7.2. Ustalenia harmonogramu prac z Zamawiającym;

7.3. Współpracy z administratorami 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

7.4. Udziału w spotkaniach z administratorami Zamawiającego.

**8.** Instruktaż

8.1. Wykonawca przeprowadzi instruktaż dla nie więcej niż 15 pracowników Zamawiającego, który przygotuje wskazanych pracowników do samodzielnej administracji i zarzadzania oprogramowaniem zainstalowanym w CB, zapozna z podstawami zarządzania środowiskiem z poziomu konsoli zarządzającej i graficznego interface DataDomain OS oraz wykonywania backupów i odtworzeń wykorzystywania skonfigurowanego CB w specyficznej infrastrukturze Zamawiającego.

8.1.1. Instruktaż zostanie przeprowadzony w języku polskim przez osoby będące trenerami producenta lub Wykonawcy oraz posiadające kwalifikacje i umiejętności potwierdzone certyfikatem producenta oferowanego rozwiązania.

8.1.2. Lista uczestników instruktażu zostanie ustalona drogą mailową z Wykonawcą po podpisaniu Umowy.

8.1.3. Instruktaż zostanie zorganizowany w czasie trwania wdrożenia rozwiązania.

8.1.4. Termin przeprowadzenia instruktażu zostanie ustalony pomiędzy Zamawiającym, a Wykonawcą.

8.1.5. Instruktaż będzie realizowany w dni robocze w godzinach 8:00-16:00 w siedzibie Zamawiającego lub zdalnie za zgodą Zamawiającego. Instruktaż może się odbyć w postaci zdalnego spotkania o ile zostaną spełnione wszystkie wymagania instruktażu.

8.1.6. Instruktaż będzie trwał minimum 3 dni robocze.

8.1.7. Harmonogramy zajęć zostaną ustalone drogą mailową z Zamawiającym.

8.1.8. Wykonawca musi posiadać autoryzację producenta w zakresie prowadzenia instruktażu z wdrożonego u Zamawiającego rozwiązania.

8.1.9. Dla uczestników instruktażu Wykonawca przygotuje środowisko testowe tożsame dla wdrożonego u Zamawiającego rozwiązania pozwalające na wykonanie ćwiczeń w warunkach możliwie zbliżonych do realnych.

8.1.10. Wykonawca zapewni dla każdego uczestnika wersję elektroniczną materiałów dydaktycznych zawierających streszczenie/omówienie wszystkich zagadnień zawartych w programie instruktażu oraz prezentacje wykorzystane podczas instruktażu.

8.1.11. Jeśli na potrzeby realizacji instruktażu powstaną materiały edukacyjne będące utworami w rozumieniu ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych będą one w ramach wynagrodzenia przewidzianego w Umowie udostępnione na licencji zapewniającej licencjobiorcy – Zamawiającemu prawo do wykorzystywania utworów zgodnie z ich przeznaczeniem na czas nieokreślony.

8.1.12. Wykonawca po zakończeniu instruktażu wystawi dla uczestników dokument/certyfikat potwierdzający odbycie instruktażu wraz z jego zakresem.

8.1.13. Zakres tematyczny instruktażu będzie zawierał się w niniejszych obszarach:



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

Zamawiający wymaga organizacji instruktażu z dwóch obszarów dla maksymalnie 15 osób:

- Obszar Cyfrowy Bunkier:
- Wymiar co najmniej 24 godziny, które mogą być dowolnie podzielone jednak całość instruktażu musi odbyć się w ciągu jednego tygodnia roboczego.
- Tematyka instruktażu musi obejmować administrację i zarządzanie oprogramowaniem zainstalowanym w CB.
- Termin instruktażu zostanie ustalony z co najmniej tygodniowym wyprzedzeniem.
- Obszar Backupu:
- Wymiar co najmniej 24 godziny, które mogą być dowolnie podzielone jednak całość instruktażu musi odbyć się w ciągu  tygodnia roboczego.
- Zakres obejmować będzie podstawy zarządzania środowiskiem z poziomu konsoli zarządzającej i graficznego interface DataDomain OS oraz wykonywanie backupów i odtworzeń.
- Termin instruktażu zostanie ustalony z co najmniej tygodniowym wyprzedzeniem.
- Dopuszcza się do wykorzystania środowisko Zamawiającego jako element instruktażu.



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