Ministerstwo Rozwoju i Technologii **Warszawa, dnia 13 grudnia 2022 r.**

Plac Trzech Krzyży 3/5

00-507 Warszawa

ZAPYTANIE OFERTOWE

dotyczące dostawy oprogramowania do zarządzania danymi stacji roboczych wraz ze wsparciem producenta na okres 36 miesięcy

I. ZAMAWIAJĄCY

Ministerstwo Rozwoju i Technologii

Plac Trzech Krzyży 3/5

00-507 Warszawa

II. PRZEDMIOT ZAMÓWIENIA

Przedmiotem zamówienia jest **dostawa oprogramowania do zarządzania danymi stacji roboczych wraz ze wsparciem producenta na okres 36 miesięcy**

III. TERMIN REALIZACJI ZAMÓWIENIA

Dostawa **oprogramowania do zarządzania danymi stacji roboczych wraz ze wsparciem producenta na okres 36 miesięcy** stanowiących przedmiot zamówienia zostanie zrealizowania w terminie do 10 dni od daty zawarcia umowy.

Wykonawca wraz z oprogramowaniem dostarczy dokument potwierdzający nabycie przez Zamawiającego prawa do dostarczonego oprogramowania **do zarządzania danymi stacji roboczych wraz ze wsparciem producenta na okres 36 miesięcy.**

IV. WYMAGANIA DOTYCZĄCE REALIZACJI ZAMÓWIENIA

Dostawa oprogramowania do zarządzania danymi stacji roboczych wraz ze wsparciem producenta na okres 36 miesięcy

Oprogramowanie zabezpieczające dane stanowiące jeden, spójny system, zarządzany z poziomu jednej konsoli. Nie dopuszcza się rozwiązań pochodzących od różnych producentów, a co za tym idzie nie całkowicie zintegrowanych pomiędzy sobą wymagających wykorzystywania różnych konsol dla zarządzania czy konfiguracji.

Zamawiający rozumie archiwizację danych, jako proces przenoszenia zasobów plikowych i pocztowych do archiwum (repozytorium dyskowe) po skopiowaniu tych zasobów system musi tworzyć skróty oraz kasować zarchiwizowane dane w pełni automatycznie. Obie funkcjonalności: kasowanie danych i tworzenie skrótów musi być dostępne co najmniej dla archiwizowanych danych plikowych z systemów Windows i Linux.

W celu weryfikacji funkcjonalności oferowanych przez proponowany system, Zamawiający zastrzega sobie możliwość wezwania do przeprowadzenia wybranych testów funkcjonalnych potwierdzających zadeklarowane funkcjonalności w ciągu 5 dni od daty wezwania. W razie odmowy przeprowadzenia testów lub gdy ich wynik będzie negatywny - Zamawiający ma prawo odrzucić proponowaną ofertę.

Wymagania techniczne dotyczące systemu:

1. System musi reprezentować architekturę trójwarstwową (serwer zarządzający, serwer medialny oraz klient). Taka architektura pozwoli na elastyczną skalowalność systemu bez względu na dynamikę przyrostu danych.
2. System nie może preferować platformy sprzętowej, nie może być profilowany 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.
3. Jeśli system 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 fizycznym (minimum 2xCPU po 12 core), klastrze active-passive czy serwerze wirtualnym w środowisku Vmware i Hyper-V.
4. Licencje muszą pozwalać na stworzenie dla serwera zarządzającego systemu wysokodostępnego z częstotliwością replikacji bazy katalogowej nie dłuższym niż 15 minut (RPO nie większe niż 15 min dla uruchomienia zapasowego serwera zarządzającego). Jeśli do stworzenia takowego systemu potrzebne są licencje replikacyjne, klastrowe, współdzielona przestrzeń dyskowa to muszą zostać dostarczone. Licencje muszą pozwalać na skonfigurowanie serwerów zarządzających oraz ich replikację dla co

najmniej trzech lokalizacji, gdzie pierwsza jest lokalizacja produkcyjną, druga i trzecia są typu standby dla serwera zarządzającego.

5. Jako opcja musi istnieć możliwość zainstalowania serwera zarządzającego na systemie operacyjnym Linux z zachowaniem możliwości replikacji bazy katalogowej i tworzeniem serwerów typu standby.
6. Proces przełączenia musi umożliwiać:
    - Przełączenie manualne inicjalizowane przez administratora
    - Przełączenie automatyczne w przypadku wykrycia awarii
7. Przełączenie serwera zarządzającego musi odbywać się w pełni automatycznie poprzez administratora, który decyduje kiedy ma ono nastąpić, przełączanie serwera zarządzającego musi być możliwe pomiędzy różnymi typami infrastruktury:
    - serwer fizyczny -> serwer fizyczny
    - serwer fizyczny -> serwer wirtualny (onpremis)
    - serwer wirtualny (onpremis) -> serwer fizyczny
    - serwer wirtualny (onpremis) -> serwer wirtualny (onpremis)
    - System musi zapewnić interfejs graficzny do zarządzania i instalacji.
8. Oprogramowanie systemu musi umożliwiać zdalne instalowanie i odinstalowywanie klienta systemu z centralnego serwera dla systemów Windows, Linux i Unix – musi być to możliwe z jednego serwera pełniącego rolę cache dla wszystkich binarii klienckich.
9. System musi zapewniać funkcjonalność odtwarzania po awarii konfiguracji serwera zarządzającego tworzeniem kopii bezpieczeństwa i archiwów.
10. System musi posiadać możliwość nieodwracalnego kasowania danych – funkcjonalność ta musi być częścią oprogramowania systemu.
11. 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.
12. 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.
13. System musi pozwalać na zarządzanie całością działania (backup, archiwizacja, backup laptopów) z jednej konsoli administracyjnej oraz także z konsoli webowej.
14. Agenci systemu muszą posiadać funkcjonalność komunikowania się poprzez jeden port TCP/IP, celem zabezpieczenia komunikacji z środowisk typu DMZ.
15. Automatyczne tunelowanie komunikacji TCP/IP pomiędzy agentami systemu – jeśli agent systemu wykryje ograniczenia w komunikacji, automatycznie zestawia połączenie tunelowe wykorzystujące tylko jeden port TCP/IP.
16. 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.
17. Komunikacja agentów systemu ze stacjami roboczymi musi odbywać się poprzez SSL – konfiguracja tego typu transferu nie może powodować konieczności instalowania dodatkowego oprogramowania.
18. System musi pozwalać na współdzielenie napędów taśmowych w środowisku sieci SAN.
19. 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 systemu 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).
20. Włączenie funkcjonalności deduplikacji na kliencie musi być możliwe dla różnych systemów operacyjnych: Windows, Linux, Unix i Macintosh.
21. 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, desktopy i laptopy) – deduplikacja musi opierać się na jednej logicznej centralnej bazie deduplikacyjnej
22. 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.
23. Deduplikacja blokowa musi obejmować dane nie tylko backupowane ale i archiwizowane, przy czym wielkość bloku nie może być większa niż 128KB.
24. System musi zapewniać wspólny stopień deduplikacji (jedna baza deduplikacyjna) dla danych czy to z backupu czy archiwizacji.
25. 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.
26. 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.

27. 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.
28. 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.
29. Na jednym serwerze systemu (na jednej instancji systemu operacyjnego) mogą być zainstalowane minimum dwie bazy deduplikacyjne pozwalające zwiększyć skalowalność systemu.
30. System musi zapewniać dostęp zintegrowany z usługą katalogową, minimum to Active Directory, a więc tak zwany „single sign on" – pojedyncze logowanie: użytkownik po zalogowaniu do domeny AD, nie potrzebuje wykonywać następnego logowania aby zarządzać systemem poprzez konsolę administracyjną.
31. System musi być odporny na tzw. „atak na wzorzec czasu": to znaczy iż przy radykalnej zmianie czasu na serwerze zarządzającym o co najmniej 1 godzinę do tyłu lub o 4 godziny do przodu względem danego czasu na serwerze – System musi automatycznie zatrzymać swoje jakiekolwiek działania aby zabezpieczyć dane przed wykasowaniem (ekspiracją).
32. 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.
33. System musi pozwalać na zarządzanie poprzez „cmd" z tym, że uruchomienie jakiejkolwiek komendy/polecenia musi zostać poprzedzone koniecznością zalogowania (autentyfikacji) do systemu, funkcjonalność musi dotyczyć dowolnej platformy (minimum Windows/Linux) i nie może polegać na konieczności instalowania czy konfigurowania dodatkowych komponentów np. SSH.
34. Komunikacja pomiędzy agentem a serwerem systemu musi opierać się na certyfikatach.
35. 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 nie tylko dla danych z laptopów/desktopów ale i dla serwerów (także dla danych plikowych i bazodanowych).
36. System musi pozwalać na skonfigurowanie mechanizmu podwójnej autentyfikacji administratora – do uruchomienia konsoli administracyjnej systemu potrzebne jest nie tylko logowanie, ale i dodatkowy tymczasowy kod wysyłany do administratora np. poprzez mail.
37. Szyfrowanie danych musi pozwalać na wybór algorytmu (minimum dwa algorytmy: Blowfish, AES) także dla danych deduplikowanych na kliencie systemu.
38. 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.
39. System musi wspierać mechanizm szyfrowania danych na napędach taśmowych LTO.
40. System musi pozwalać na ustawianie haseł dostępu do nośników tzw: media password.
41. System musi pozwalać na integrację z zewnętrznymi repozytoriami do przechowywania kluczy szyfrującym zgodnymi z KMIP – minimum dla:
    - Fortanix Data Security Manager
    - HashiCorp Vault
    - IBM Security Key Lifecycle Manager (SKLM)
    - Safenet
    - StorMagic SvKMS
    - Thales CipherTrust Manager
    - Vormetric
    - Amazon Web Services (AWS) key management service
    - Microsoft Azure Key Vault
42. System musi umożliwiać składowanie kopii bazy katalogowej w chmurze producenta oprogramowania, funkcjonalność ta musi być w cenie produktu i pozwalać na automatyczne składowanie kopii bazy.
43. System musi mieć wbudowane mechanizmy zabezpieczające przed złośliwym oprogramowaniem (Ransomware), minimum to:
    - zabezpieczenie ścieżek dostępu do danych składowanych (kopii backupowych) na dyskach – tylko procesy systemu mogą zapisywać i modyfikować dane;
    - 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;
    - 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;
    - możliwość definiowania kierunku inicjalizowania komunikacji sieciowej pomiędzy komponentami systemu backupowego;

- możliwość zablokowania zmiany retencji (czas przechowywania kopii backupowych) na krótszą dla kopii backupowych składowanych na dowolnych typach nośników w tym na dyskach i taśmach – wbudowany w system mechanizm WORM dla dowolnych typów storage gdzie mogą być składowane kopie backupowe.

44. System musi posiadać rozbudowany system powiadamiania o zdarzeniach poprzez email.
45. System musi posiadać zaawansowane mechanizmy exportu i analizy logów poprzez:
    - Syslog serwer
    - Elasticsearch
46. Automatyczne monitorowanie stanu systemu poprzez wiadomości SMS na urządzeniach mobilnych i telefonach.
47. System musi posiadać rozbudowany system raportowania dla administratorów, minimalny zestaw dostępnych raportów to:
    - raport zmian/wzrostu środowiska systemu;
    - raport wykorzystania licencji;
    - raport wykonanych zadań backupowych;
    - raporty obciążenia serwerów backupowych – minimum monitorowanie użycia CPU i pamięci RAM.
48. System musi mieć możliwość automatycznego wysyłania dowolnych raportów do wybranych użytkowników poprzez mail.
49. System musi mieć możliwość automatycznego zapisywania raportów w formacie minimum: PDF, HTML i CSV.
50. System musi pozwalać na definiowanie alertów per zadanie backupowe lub zadanie odtwarzania danych przy spełnieniu minimum kryteriów:
    - czas zadania dłuższy niż zadany;
    - ilość danych większa niż ….;
    - ilość danych mniejsza niż ….;
    - ilość nie zbackupowanych plików większa niż…;
    - ilość nie zbackupowanych plików większa niż …%;
    - wielkość backupowanych danych większa niż …
51. Notyfikacje alertów muszą być wysyłane minimum poprzez mail.
52. Raport spełnienia wymogów SLA dla parametrów:
    - ilości dodatkowych kopii backupowych;
    - RTO;
    - RPO;
53. System musi zapewniać funkcjonalność wznawiania zadań backupowych.
54. System musi zapewniać funkcjonalność równoległego wykonywania kopii danych backupowanych – inline copy (tego samego zestawu danych pojedynczego klienta) na minimum dwa docelowe urządzenia przechowywania danych.
55. 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.
56. Funkcjonalność multistreamingu musi być dostępna dla deduplikacji bez względu czy następuje na kliencie czy na serwerze systemu.
57. System musi zapewniać funkcjonalność multipleksowania kilku strumieni danych na nośniku taśmowym – tzw. multiplexing. Wydajny zapis wielu strumieni danych na taśmy bez pośrednictwa dysków.
58. System musi posiadać możliwość wykonywania backupu pełnego, przyrostowego, różnicowego oraz syntetycznego.
59. System musi oferować funkcjonalność backupu blokowego, polegającego na tym, iż agent buduje własną bazę zmian bloków danych, przez co backup przyrostowy nie wymaga odczytu całych plików tylko zmienionych bloków wielokrotnie przyspieszając backup. Funkcjonalność ta musi być dostępna dla backupu danych plikowych.
60. System musi posiadać funkcję szyfrowania i kompresji danych transmitowanych przez LAN, możliwość wykorzystania szyfrowania i kompresji musi być dostępna w dowolnej kombinacji.
61. 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.
62. System musi posiadać zintegrowane w systemie mechanizmy indeksowania pełnokontekstowego i wyszukiwania danych. Indeksowaniu powinny podlegać dane zbackupowane i zarchiwizowane już znajdujące się w systemie.
63. System musi realizować funkcjonalność weryfikacji wykonanych kopii.
64. System musi umożliwiać wykorzystanie funkcjonalności Bare Metal Restore dla odtwarzania systemu po awarii, wsparcie musi być dostępne dla systemów:
    - Windows;
    - Linux: Debian/Oracle Linux/RHEL/CentOs/SuSe/Ubuntu.

65. System musi umożliwiać analizę logów z systemów zewnętrznych, na bazie zdefiniowanych kryteriów powinien generować alarmy lub akcje. Minimalne wsparcie to: Windows Event Log.
66. System musi wspierać wykonanie kopii na systemach klasy Windows, Linux i Unix.
67. System musi umożliwiać uruchamianie skryptów przed i po backupie, z tym iż musi posiadać mechanizm definiowania konta użytkownika na którym te skrypty byłyby uruchamiane. Mechanizm ten musi być centralnie zarządzany poprzez konsolę administracyjną. Niedopuszczalna jest konieczność np. zmiany konta serwisowego dla danego agenta – konta serwisowe muszą być centralnie definiowane i zarządzane.
68. System musi zapewniać backup laptopów i desktopów – funkcjonalność ta musi być w pełni zintegrowana z systemem (ta sama konsola, to samo repozytorium danych, ta sama deduplikacja) o funkcjonalnościach:
    - portal samoobsługowy musi być dostępny poprzez dowolną przeglądarkę sieci Internet minimum: Edge, Chrome, Opera, Mozilla, Safari;
    - system musi umożliwiać backup laptopów czy desktopów z systemami Windows, Linux i Macintosh;
    - dostęp do danych zbackupowanych z laptopów czy desktopów musi być możliwy z urządzeń mobilnych poprzez dedykowanego klienta minimum dla IOS i Android;
    - dla backupu laptopów i desktopów system backupowy musi oferować dedykowanego agenta, który pozwala skonfigurować zadanie backupowe tak by było wykonane w przedziale czasowym bez podawania konkretnej daty czy czasu jego uruchomienia, agent nie może tworzyć kopii danych na lokalnych zasobach stacji/laptopa;
    - system musi zapewniać współdzielenie plików pochodzących z backupu laptopów i desktopów z użytkownikami z domeny AD oraz z użytkownikami spoza domeny;
    - Geolokacja – system musi w konsoli dla użytkownika pokazywać ostatnią lokalizację laptopa lub desktopa;
    - każdy użytkownik desktopa czy laptopa musi posiadać możliwość zarządzania własnymi danymi, minimalna oczekiwana funkcjonalność to:
        - ✓ odtwarzanie własnych danych;
        - ✓ uruchomienie backupu;
        - ✓ wstrzymanie backupu;
        - ✓ możliwość zdefiniowania innego okna backupowego;
        - ✓ możliwość monitorowania postępu działania zadania;
        - ✓ możliwość przeglądania danych ze stacji roboczej czy laptopa poprzez dedykowanego klienta dla urządzeń mobilnych, a więc użytkownik posiadając jedynie urządzenie mobilne może nie tylko odczytywać dane z backupowej kopii ale także przeglądać dane na stacji roboczej nawet w momencie gdy jest poza siedzibą firmy – korzysta jedynie z dostępu do internetu (do przeglądania danych nie jest potrzebne żadne dodatkowe połączenie VPN);
    - wirtualny dysk - system musi oferować funkcjonalności jak:
        - ✓ możliwość synchronizacji wybranego katalogu/foldera z stacji roboczej celem automatycznego backupu danych w nim zapisanych (backup ciągły);
        - ✓ możliwość przesłania katalogów i plików ręcznie;
        - ✓ zarządzanie poprzez przeglądarkę i dedykowaną aplikację na urządzeniach minimum iOS i Android;
            - zabezpieczenie przed kradzieżą, system musi posiadać możliwość zdalnego zaszyfrowania danych w przypadku kradzieży laptopa, to znaczy iż w przypadku utraty urządzenia administrator lub użytkownik włącza opcję szyfrującą i jeśli urządzenie pojawi się w sieci, dane zostaną automatycznie zaszyfrowane;
            - możliwość archiwizowania danych plikowych na stacji roboczej: jeśli dane pliki spełniają kryteria archiwizacyjne to dany pliki zostaje skasowany albo zamieniony na skrót (stub);
            - deduplikacja blokowa i szyfrowanie wykonywane na kliencie (stacji roboczej/laptopie);
            - możliwość szyfrowania nie tylko kopii backupowych ale całej transmisji pomiędzy desktopem/laptopem a systemem backupowym;
            - możliwość backupu z wykorzystaniem szyfrowanego tunelu niezależnie czy desktop/laptop jest w sieci wewnętrznej firmy czy łączy się zdalnie przez sieć internet, bez korzystania z rozwiązań typu VPN;
69. System musi umożliwiać pełnokontekstowe indeksowanie treści danych dla wybranych typów plików, z backupu stacji roboczych, indeksacja musi odbywać się dla danych znajdujących się już w systemie.
70. System musi umożliwiać przeprowadzanie wielu wyszukiwań (eDiscovery) i zbierać wszystkie wyniki w jednej lokalizacji.
71. System musi posiadać zaawansowaną funkcjonalność analizy zasobów plikowych minimum o funkcjonalnościach:
    - detekcja powtarzających się zasobów;
    - raportowanie praw dostępu do plików;
    - raportowanie i analiza dostępu do zasobów i ich modyfikacji;
    - możliwość kasowania plików z zasobów .

72. System musi pozwalać na wyszukiwanie danych wrażliwych (np. numery PESEL) i pozwalać osobie uprawnionej nie tylko na raportowanie takich zdarzeń ale także umożliwiać kasowanie plików nie tylko z systemów produkcyjnych ale i z kopii backupowej.
73. Musi istnieć możliwość zarządzania systemem poprzez Windows PowerShell.
74. Monitorowanie i alertowanie klientów systemu którzy są trybie offline, a więc komunikacja z nimi przez system backupowy nie jest możliwa.
75. System musi posiadać integrację z ServiceNow o funkcjonalnościach:
    - dedykowany plugin do ServiceNow;
    - możliwość zgłaszania zdarzeń backupowych i odtworzeniowych bezpośrednio z konsoli Service Now.
76. Możliwość zwiększenia bezpieczeństwa systemu poprzez integrację z CyberArk.
77. Musi istnieć możliwość wskazania klucza szyfrującego (Bring Your Own Key – BYOK), który będzie wykorzystywany do szyfrowania kopii backupowych.
78. Możliwość anonimizacji danych wrażliwych (data masking) minimum dla logów systemu wysyłanych np. do wsparcia.
79. 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.

Wymogi dla licencjonowania

1. Niedopuszczalne jest aby licencjonowanie było zależne od ilości składowanych danych (kopii backupowych) na dowolnych nośnikach (np. dysk, taśma VTL…) czy to z deduplikacją czy bez.
2. Niedopuszczalne jest aby licencjonowanie było zależne od ilości komponentów środowiska backupowego, które będą wykorzystywane w procesie backupu czy odtwarzania danych.
3. Zaoferowane licencje nie mogą ograniczać wielkości przestrzeni do składowania danych czy replik ich do innych lokalizacji. Jakakolwiek rozbudowa przestrzeni dyskowej czy to w siedzibie podstawowej czy innej nie może wymagać zakupu jakichkolwiek licencji dla systemu.
4. Oferowane licencje oraz architektura systemu musi pozwalać na backup danych na:
    - nielimitowana ilość bibliotek taśmowych i napędów fizycznych
    - nielimitowaną przestrzeń w systemach chmurowych (minimum: AWS, Azure, Google)
    - nielimitowana przestrzeń dyskową (DAS, NAS) podłączona do systemu
5. W przypadku wielu lokalizacji licencje muszą pozwalać na nielimitowaną replikację danych po deduplikacji pomiędzy lokalizacjami.
6. Do dostarczonego systemu wraz z licencjami wymagane jest 36 miesięczne wparcie producenta (pierwsza i druga linia wsparcia świadczona w języku polskim) zapewniające wsparcie techniczne w trybie od 8.00 do 16.00 przez 5 dni roboczych oraz dostęp do bezpłatnych ewentualnych poprawek i uaktualnień.
7. Zaoferowane licencje na system muszą zapewnić backup danych ze środowiska o wielkości:
    - Środowisko backupu stacji roboczych - Ilość użytkowników podlegających backupowi – minimum 150.

Wymogi dla wdrożenia

W ramach dostarczenia systemu wymagana jest także usługa wdrożenia systemu zgodnie ze standardami producenta. Usługa wdrożenia musi zawierać:

1. wsparcie w wyskalowaniu środowiska produkcyjnego zgodnie z wytycznymi producenta;
2. instalację oprogramowania serwera zarządzającego oraz niezbędnych usług pomocniczych (proxy itp.) na infrastrukturze Zamawiającego zgodnie z wytycznymi producenta;
3. wsparcie w wytworzeniu procedury instalacji agentów oprogramowania z wykorzystaniem narzędzi Zamawiającego lub dostarczonymi wraz z systemem;
4. przeprowadzenie wstępnej instalacji na min. 10 stacjach roboczych wspólnie z administratorami Zamawiającego na bazie wytworzonej procedury instalacji;
5. weryfikacja wydajności, stabilności i poprawności skalowania środowiska w odstępie min. 2 tygodni od wykonania pierwszych kopii zapasowych;
6. sporządzenie dokumentacji powdrożeniowej.

V. DODATKOWE INFORMACJE:

1. Oferta powinna zostać podpisaną przez osobę uprawnioną do reprezentacji Wykonawcy.
2. **Termin składania ofert wyznaczony został na 16.12.2022 r. do godziny 12:00.**
3. Wykonawca wraz z ofertą powinien złożyć oświadczenie składane z art. 7 ust. 1 ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego. Oświadczenie musi być podpisane przez osobę/y uprawnioną/e do reprezentacji Wykonawcy (w przypadku reprezentacji na podstawie pełnomocnictwa należy załączyć odpowiednie dokumenty umożliwiające weryfikację upoważnienia).