ZAPYTANIE OFERTOWE

w postępowaniu prowadzonym zgodnie z zasadą konkurencyjności

Zamówienie w ramach projektu p.n. *„Wdrożenie do firmy Paged Plywood S.A. kompletnego cyberfizycznego systemu, umożliwiającego cyfryzację i robotyzację produkcji sklejki i wprowadzenie założeń przemysłu 4.0. na rzecz zwiększenia odporności do działania w warunkach kryzysowych”* współfinansowane z **KRAJOWEGO PLANU ODBUDOWY, A2.1.1 – Inwestycje wspierające robotyzację i cyfryzację w przedsiębiorstwach**

PRZEDMIOT ZAMÓWIENIA:

Kompleksowy system do tworzenia kopii zapasowych
oraz ochrony przed atakami szyfrującymi dane

ZAMAWIAJĄCY:

Paged Plywood S.A.
14-300 Morąg, ul. Mazurska 1,
NIP 7411378488, REGON 510445569

System będzie obejmował Zakład Produkcji Sklejki w Piszu i Zakład Produkcji Sklejki Morągu

1. OPIS PRZEDMIOTU ZAMÓWIENIA

kody CPV:

- 48820000-2 – Serwery
- 48000000-8 – Pakiety oprogramowania i systemy informatyczne
- 72268000-1 – Usługi dostawy oprogramowania
- 72260000-5 – Usługi w zakresie oprogramowania

Załącznik „Specyfikacja Istotnych Warunków Zamówienia” opisuje szczegółowe wymagania dotyczące zamawianego systemu. W szczególności zapytanie obejmuje:

- **system kopii zapasowych (oprogramowanie) zabezpieczające dane;**

- **urządzenia dyskowe do przechowywania kopii zapasowych danych;**
- **serwer skanowania kopii zapasowych;**
- **serwery zarządzania i przesyłania danych;**
- **wdrożenie, przeszkolenie i wsparcie powdrożeniowe**.

W przypadku, gdzie Zamawiający posługuje się w opisie przedmiotu zamówienia, we wszystkich dokumentach i załącznikach opisujących przedmiot zamówienia nazwami konkretnych producentów, nazwami konkretnych produktów, znakami towarowymi, patentami czy pochodzeniem, należy to traktować jedynie jako pomoc w opisie przedmiotu zamówienia – mają one jedynie przybliżyć wymagania, których nie można było opisać przy użyciu dostatecznie dokładnych i zrozumiałych określeń. W przypadku pozycji oznaczonych określeniem „lub równoważnym" dopuszcza się użycie produktu podobnego, który spełni minimalne standardy jakościowe, parametry techniczne, warunki docelowego przeznaczenia oraz funkcji i walorów użytkowych produktu wskazanego z nazwy.
W każdym przypadku dopuszcza się możliwość zastosowania materiałów, komponentów równoważnych wobec wskazanych w opisie przedmiotu zamówienia oraz załącznikach pod warunkiem zachowania ich zgodności z planowanym przeznaczeniem i obowiązującymi przepisami, które spełniają minimalne standardy jakościowe, parametry techniczne, warunki docelowego przeznaczenia oraz funkcje i walory użytkowe.
W związku z przyjętym harmonogramem realizacji inwestycji, w przypadku pytań lub wątpliwości co do przedmiotu zamówienia, prosimy o kierowanie zapytań najpóźniej do pięciu dni przed terminem składania ofert.

2. WARUNKI UDZIAŁU W POSTĘPOWANIU

Oferty mogą składać Wykonawcy, którzy:

1. dysponują potencjałem technicznym, koniecznym do należytego wykonania zamówienia;
2. zrealizują umowę maksymalnie 18 tygodni od dnia podpisania umowy;
3. znajdują się w sytuacji ekonomicznej i finansowej zapewniającej realną możliwość wykonania zamówienia;
4. posiadają wykwalifikowaną kadrę gotową do realizacji zamówienia;
5. posiadają niezbędną wiedzę i doświadczenie oraz zdolności techniczne i organizacyjne umożliwiające prawidłowe wykonanie przedmiotu zamówienia;
6. nie posiadają powiązań osobowych ani kapitałowych z Zamawiającym – przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między Beneficjentem lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Beneficjenta lub osobami wykonującymi w imieniu Beneficjenta czynności związanych z przygotowaniem i przeprowadzeniem procedury wyboru wykonawcy a wykonawcą, polegające w szczególności na:
   - uczestniczenie w spółce jako wspólnik spółki cywilnej lub spółki osobowej;
   - posiadanie co najmniej 10% udziałów lub akcji (o ile niższy próg nie wynika z przepisów prawa);
   - pełnienie funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika;
   - pozostawanie w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, lub w linii bocznej do drugiego stopnia, lub związanie z tytułu przysposobienia, opieki lub kurateli albo pozostawanie we wspólnym pożyciu z wykonawcą, jego zastępcą prawnym lub członkami organów zarządzających lub organów nadzorczych wykonawców ubiegających się o udzielenie zamówienia;
   - pozostawanie z wykonawcą w takim stosunku prawnym lub faktycznym, że istnieje uzasadniona wątpliwość co do ich bezstronności lub niezależności w związku z postępowaniem o udzielenie zamówienia.

3. KRYTERIA OCENY OFERTY

Oferty będą oceniane wg następujących kryteriów:

1. 75% – cena;
2. 25% – termin dostawy i realizacji.

Z postępowania zostaną wykluczone oferty, które:

1. nie spełniają warunków umieszczonych w zapytaniu ofertowym, w tym w specyfikacji istotnych warunków zamówienia;
2. pochodzą od wykonawców mających powiązania osobowe lub kapitałowe z Zamawiającym;
3. zawierają istotne błędy w obliczeniu ceny lub cena oferty jest rażąco niska – w takiej sytuacji Zamawiający może poprosić o uzupełnienie oferty o dokumenty potwierdzające możliwość realizacji oferty w tej cenie;
4. zostaną złożone po wskazanym terminie;
5. będą zawierały zbyt długi termin realizacji uniemożliwiający finansowanie w ramach projektu KPO.

4. OPIS SPOSOBU PRZYZNAWANIA PUNKTACJI ZA SPEŁNIENIE DANEGO KRYTERIUM OCENY OFERTY

Kryterium ceny uwzględniające wszystkie niewykluczone oferty, zgodnie ze wzorem:

$$C_{\%} = \left(1 - \frac{C_n - C_{min}}{C_{max} - C_{min}}\right) * 75\%$$

w szczególności: najniższa cena 75%, najwyższa cena 0%.

Termin dostawy i realizacji liczony od dnia podpisania umowy:

- 25% – do 6 tygodni;
- 20% – 6-8 tygodni;
- 15% – 8-10 tygodni;
- 10% – 10-12 tygodni;
- 5% – 12-14 tygodni;
- 0% – powyżej 14 tygodni.

5. MIEJSCE ORAZ TERMIN SKŁADANIA OFERT

Oferty prosimy składać do 29 lipca 2025 r. na adresy:

- it@paged.pl
- sekretariat@paged.pl

6. INFORMACJA O MOŻLIWOŚCI SKŁADANIA OFERT CZĘŚCIOWYCH

Zamawiający nie dopuszcza możliwości składania ofert częściowych.

INFORMACJĘ O PLANOWANYCH ZAMÓWIENIACH UZUPEŁNIAJĄCYCH

Zamawiający nie planuje zamówień uzupełniających.

7. TERMIN REALIZACJI UMOWY

Maksymalnie 18 tygodni od dnia podpisania umowy.

8. ISTOTNE POSTANOWIENIA UMOWY I WARUNKI ZMIANY ISTOTNYCH POSTANOWIEŃ UMOWY

Zamawiający wymaga, aby Wykonawca, którego oferta zostanie uznana za najkorzystniejszą, zawarł umowę zgodnie z treścią zapytania. Wykonawca ma prawo zaproponować wzór umowy stosowany w praktyce handlowej. Zamawiający dopuszcza wypłatę zaliczki na poczet realizacji zamówienia w kwocie uzgodnionej z Wykonawcą nie wyższą niż 50% ceny ujawnionej przez Wykonawcę w ofercie.

9. WARUNKI EWENTUALNEGO ODSTĄPIENIA OD ZAWARCIA UMOWY

W przypadku gdy zaoferowana cena przekracza kwotę środków przeznaczonych przez Zamawiającego na realizację zamówienia Zamawiający może unieważnić postępowanie i odstąpić od podpisania umowy.

10. ZAŁĄCZNIKI

Oferty prosimy składać wraz z wypełnionymi załącznikami.

Załącznik 1 – Formularz oferty

W odpowiedzi na Zapytanie Ofertowe dotyczące
Kompleksowy system do tworzenia kopii zapasowych oraz ochrony przed atakami szyfrującymi dane
składamy poniższą ofertę:

Dane oferenta	
Nazwa	
Adres	
NIP / REGON	
Nr KRS lub CEIDG	
Nr rejestrowy dla kraju innego niż POLSKA	
Dane osoby kontaktowej	
Imię i nazwisko	
Adres e-mail	
Telefon	
Określenie do kryteriów wyboru ofert	
Wartość oferty netto w PLN	
Termin realizacji liczony w tygodniach od daty podpisania umowy	

Załącznik 2 – Oświadczenie o spełnieniu wszystkich warunków udziału w postępowaniu

1. Dysponuję potencjałem technicznym, koniecznym do należytego wykonania zamówienia.
2. Znajduję się w sytuacji ekonomicznej i finansowej zapewniającej realną możliwość wykonania zamówienia.
3. Posiadam wykwalifikowaną kadrę gotową do realizacji zamówienia.
4. Posiadam niezbędną wiedzę i doświadczenie oraz zdolności techniczne i organizacyjne umożliwiające prawidłowe wykonanie przedmiotu zamówienia.

Załącznik 3 – Oświadczenie o braku powiązań osobowych i kapitałowych

Oświadczam(y), że nie jestem(eśmy) powiązani z Zamawiającym osobowo lub kapitałowo.

……

data i podpis przedstawiciela Wykonawcy (dotyczy wszystkich 3 załączników)

Załącznik 4 – Specyfikacja istotnych warunków zamówienia (SIWZ)

SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA

Wszystkie poniższe wymagania opisują minimalne parametry, które musi spełniać oferta.

1. **Wymagania ogólne**

    1. system ma działać bezprzerwowo 24/h na dobę 7 dni w tygodniu;
    2. kopie zapasowe powinny być zapisywane lokalnie oraz co najmniej w 1 dodatkowej lokalizacji;
    3. w przypadku awarii pojedynczego urządzenia reszta infrastruktury powinna nadal działać, a odzyskanie / przywrócenie kopii powinno być możliwe z urządzenia w innej lokalizacji;
    4. aktualizacje oprogramowania („software"), w tym oprogramowania układowego („firmware") powinno odbywać się automatycznie w taki sposób, aby urządzenia w każdej lokalizacji były aktualizowane w innych przedziałach czasu;
    5. w razie potrzeby wsparcie techniczne powinno być udzielane najpóźniej w następnym dniu roboczym po zgłoszeniu zapotrzebowania;
    6. w ramach gwarancji naprawa lub wymiana urządzeń powinna odbywać się w ciągu 14 dni roboczych.

2. **System kopii zapasowych (oprogramowanie) zabezpieczający dane**

Pojęcie system wskazuje na rozwiązanie zabezpieczające dane stanowiące jedno, spójne rozwiązanie, zarządzane z poziomu jednej konsoli. Nie dopuszcza się rozwiązań pochodzących od różnych producentów, a co za tym idzie niezintegrowanych całkowicie 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, oraz wiadomości e-mail z systemów Exchange On premise i Exchange Online – w zakresie tych funkcjonalności.
Jeśli przy danym punkcie wymogu występuje informacja „jako opcja" oznacza to iż zaproponowany system posiada daną funkcjonalność, a jej uruchomienie może wymagać zakupu dodatkowych licencji – Zamawiający nie oczekuje oferty na nią a jedynie chce mieć możliwość w przyszłości rozbudowy o tę funkcjonalność.
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. Odmowa przeprowadzenia testów lub ich wynik negatywny stanowią podstawę do odrzucenia oferty przez Zamawiającego.

Wymogi podstawowe

1. Rozwiązanie musi reprezentować architekturę trójwarstwową (serwer zarządzający, serwer medialny oraz klient), taka architektura pozwoli na elastyczną skalowalność rozwiązania bez względu na dynamikę przyrostu danych.
2. 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.
3. Jeśli system korzysta z bazy danych to wszelkie potrzebne licencje muszą być dostarczone i stanowić integralną część oferty, z tym że licencje dla silnika bazodanowego muszą pozwalać na zainstalowanie go: na serwerze fizycznym (minimum 2xCPU po 16 rdzeni każdy), klastrze active-passive, serwerze wirtualnym w środowisku VMware lub Hyper-V.

4. 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 min 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 lokalizacją 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. Jako opcja musi istnieć możliwość testowania (walidacji) odtwarzania serwera zarządzającego w chmurze producenta w celu weryfikacji możliwości DR (data recovery) w przypadku jego awarii.
7. Proces przełączenia serwera zarządzającego musi umożliwiać:
    - przełączenie automatyczne inicjalizowane przez administratora;
    - przełączenie automatyczne (bezobsługowe) w przypadku wykrycia awarii (w przypadku awarii serwera zarządzającego system automatycznie wykrywa awarie i przełącza działanie systemu na serwer zapasowy – standby, bez konieczności jakiejkolwiek interwencji administratora).
8. Przełączenie serwera zarządzającego musi odbywać się w pełni automatycznie poprzez administratora, który decyduje kiedy ma ono nastąpić, przełączanie serwera zarządzającego musi być możliwe pomiędzy takimi samymi, bądź różnymi typami infrastruktury:
    - z/na serwer fizyczny;
    - z/na serwer wirtualny (on premise);
    - z/na serwer wirtualny (w chmurze, np. AWS, Azure, Google).
9. Mechanizm przełączania serwera zarządzającego musi pozwalać na wybór trybu co najmniej spośród:
    - „Test failover” (testowanie mechanizmu przełączania);
    - „Failover” (produkcyjne przełączenie działania na serwer standby);
    - „Maintenance failover” (przełączenie w celu np. aktualizacji oprogramowania).
10. Rozwiązanie musi zapewnić interfejs graficzny do zarządzania i instalacji.
11. Oprogramowanie 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 niezbędnych plików binarnych/instalacyjnych.
12. System musi zapewniać funkcjonalność odtwarzania po awarii konfiguracji serwera zarządzającego tworzeniem kopii bezpieczeństwa i archiwów.
13. System musi posiadać możliwość nieodwracalnego kasowania danych – funkcjonalność ta musi być częścią oprogramowania i musi pozwalać na wyczyszczenie przestrzeni dyskowych (zamazanie) tak, aby nie było możliwości odzyskania tych danych nawet przy użyciu specjalistycznego sprzętu i oprogramowania.
14. Administrator systemu musi mieć możliwość wybrania i skasowania plików z danego backupu (np. plików wirusa), tak aby te pliki nie odtwarzały się przy przywracaniu tej kopii.
15. 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.
16. System musi pozwalać na składowanie danych na taśmach celem przechowywania długoterminowego. Składowane dane na taśmach muszą być w formie niezdeduplikowanej (nawodnione) po to, by była możliwość odtwarzania ich bezpośrednio, a więc bez konieczności pośrednictwa dysków, buforów czy importu.
17. System musi pozwalać na zarządzanie całością działania systemu (backup, archiwizacja, odtwarzanie; backup laptopów, maszyn wirtualnych, baz danych) z jednej konsoli administracyjnej.

18. Agenci systemu muszą posiadać funkcjonalność komunikowania się poprzez jeden port TCP/IP, celem zabezpieczenia komunikacji ze środowisk typu DMZ.
19. Automatyczne tunelowanie komunikacji TCP/IP pomiędzy agentami systemu – jeśli agent systemu wykryje ograniczenia w komunikacji, wtenczas automatycznie zestawia połączenie tunelowe wykorzystujące tylko jeden port TCP/IP.
20. 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).
21. System musi umożliwiać konfigurację, którymi kartami sieciowymi ma przebiegać komunikacja i transfer danych, wybór interfejsu musi odbywać się co najmniej poprzez nazwę domeny oraz adresację IP.
22. System musi pozwalać na współdzielenie napędów taśmowych w środowisku sieci SAN.
23. System musi umożliwić przechowywanie jedynie unikalnych bloków danych, tzw. deduplikację. 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 musi być możliwa poprzez dodanie dodatkowej przestrzeni do składowania danych poprzez dodanie dysków, półki dyskowej a nie przez wymianę urządzenia czy serwera).
24. Włączenie funkcjonalności deduplikacji na kliencie musi być możliwe dla różnych systemów operacyjnych: Windows, Linux, Unix i Mac OS.
25. Logiczna globalna deduplikacja – system musi oferować deduplikację globalną, co oznacza że niezależnie z jakich klientów dane będą deduplikowane (serwery fizyczne, hosty wirtualne, bazy i aplikacje) – deduplikacja musi opierać się na jednej logicznej centralnej bazie deduplikacyjnej.
26. 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.
27. Deduplikacja blokowa musi obejmować dane nie tylko backupowane ale i archiwizowane, przy czym wielkość bloku nie może być większa niż 128KB.
28. System musi zapewniać wspólny stopień deduplikacji (jedna baza deduplikacyjna) dla danych czy to z backupu czy archiwizacji.
29. 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.
30. 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.
31. System musi składować dane po deduplikacji (kopie backupowe) na storage obiektowym zgodnym z S3 czy to w środowisku lokalnym (on premise) czy w chmurze (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 wyłącznie w zakresie unikalnych bloków danych.

32. 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.
33. 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.
34. Na jednym serwerze systemu (na jednej instancji systemu operacyjnego) mogą być zainstalowane minimum dwie bazy deduplikacyjne pozwalające zwiększyć skalowalność systemu.
35. 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 logowania, aby zarządzać systemem poprzez konsolę administracyjną, przy czym musi istnieć możliwość uruchomienia i wymuszenia logowania wieloskładnikowego (MFA).
36. Możliwość wykorzystywania różnych dostarczycieli tożsamości (identity providers - IdP), co najmniej: OKTA, Azure, OneLogin z wykorzystaniem protokołu SAML.
37. System musi być odporny na tzw. „atak na wzorzec czasu", tzn. że przy radykalnej zmianie czasu na serwerze zarządzającym System musi automatycznie zatrzymać co najmniej proces kasowania (ekspiracji) kopii backupowych generując odpowiednie alerty do czasu potwierdzenia tej zmiany przez administratora.
38. 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.
39. Komunikacja pomiędzy agentem a serwerem systemu musi opierać się na certyfikatach.
40. 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 co najmniej dla danych z laptopów/desktopów.
41. 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.
42. Szyfrowanie danych musi pozwalać na wybór algorytmu (minimum dwa algorytmy: Blowfish, AES) także dla danych deduplikowanych na kliencie systemu.
43. 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.
44. System musi wspierać mechanizm szyfrowania danych na napędach taśmowych LTO.
45. System musi pozwalać na integrację z zewnętrznymi repozytoriami do przechowywania kluczy szyfrujących zgodnymi z KMIP – minimum dla:
    - AWS CloudHSM;
    - 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.

46. 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.
47. System musi mieć wbudowane mechanizmy zabezpieczające przed złośliwym oprogramowaniem (Ransomware), minimum to:
    - dedykowany dashboard będący częścią konsoli administracyjnej systemu do identyfikacji i zarządzania zagrożeniami, pozwalający administratorowi na działania proaktywne lub reaktywne w momencie wykrycia zagrożenia;
    - monitorowanie nietypowych zachowań systemu backupowego obejmującego obszary:
        i. czyszczenia bazy deduplikacyjnej (DDB),
        ii. zdarzeń w Systemie (events),
        iii. ilości nieudanych zadań,
        iv. ilości zadań czekających,
        v. ilości zadań zakończonych sukcesem,
        vi. konsoli monitorującej zadania,
        vii. czasu trwania zadań;
    - zabezpieczenie ścieżek dostępu do danych składowanych (kopii backupowych) na dyskach – tylko procesy systemu mogą zapisywać i modyfikować dane;
    - jako opcja monitorowanie nietypowych aktywności na serwerach plikowych;
    - monitorowanie nietypowych aktywności na serwerach za pomocą metody: Honeypot (plików pułapek/wabików) – system cyklicznie i automatycznie sprawdza czy pliki pułapki nie były modyfikowane;
    - jako opcja monitorowanie możliwego zagrożenia dotyczącego zaszyfrowania plików na serwerach;
    - jako opcja monitorowanie różnych typów plików i weryfikowanie czy typ pliku jest zgodny i czytelny z nagłówkiem tego pliku (detekcja uszkodzeń plików czy ich zaszyfrowania);
    - monitorowanie klientów Systemu i ostrzeganie 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; 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 / gateways), przez które wykonywana jest komunikacja pomiędzy modułami systemu backupowego, w szczególności pomiędzy serwerem zarządzającym i serwerem mediów czy serwerem z dowolnym agentem backupowym;
    - możliwość definiowania kierunku inicjalizowania komunikacji sieciowej pomiędzy komponentami systemu backupowego;
    - 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;
    - wsparcie dla mechanizmu WORM dla macierzy obiektowych min: Hitachi Vantara HCP i storage obiektowego w chmurze minimum: Azure, AWS, Google;
    - MFA (Multi Factor Authentication) - uwierzytelnianie wieloskładnikowe;

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

48. Identyfikacja złośliwego oprogramowania i zapobieganie ponownej infekcji dla backupów plikowych, która skanuje pliki kopii zapasowych wykorzystując różne techniki: File Entropy, SIM Hash, Signature o funkcjonalnościach minimum:
    - częstotliwość aktualizacji silnika skanującego nie mniejsza niż co 24 godziny wykonywana automatycznie;
    - manualny lub automatyczny wybór kopii backupowych zasobów plikowych do skanowania;
    - wykrywanie zagrożeń typu malware;
    - analiza z backupowanych plików pod kątem zaszyfrowania;
    - automatyczne blokowanie zainfekowanych plików z kopii backupowych przed odtwarzaniem;
    - możliwość detekcji i odtwarzania danych historycznych nie zainfekowanych;
    - raportowanie i zarządzanie komponentem poprzez konsolę administracyjna systemu backupowego;
    - skanowanie danych z pierwszej (podstawowej) lub drugiej kopii backupowej.
49. Identyfikacja złośliwego oprogramowania i zapobieganie ponownej infekcji dla kopii backupowych maszyn wirtualnych, która skanuje zawartość dysków z backupowanych maszyn wirtualnych różne techniki: File Entropy, SIM Hash, Signature o funkcjonalnościach minimum:
    - częstotliwość aktualizacji silnika skanującego nie mniejsza niż co 24 godziny wykonywana automatycznie;
    - manualny wybór maszyny wirtualnej z kopii backupowej;
    - skanowanie musi odbywać na odtworzonej maszynie wirtualnej;
    - raportowanie i zarządzanie komponentem poprzez konsolę administracyjna systemu backupowego;
    - skanowanie danych z pierwszej (podstawowej) lub drugiej kopii backupowej.
50. Wszelkie działania w systemie, także działania użytkowników końcowych muszą być logowane i przechowywane.
51. Integracja z systemami SOAR minimum: Microsoft Sentinel, Cortex Xsoar (dedykowana wtyczka dla tych systemów).
52. System musi posiadać zaawansowane mechanizmy exportu i analizy logów poprzez:
    - Syslog serwer;
    - Splunk (dedykowana wtyczka do analizy danych).
53. 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.
54. System musi mieć możliwość automatycznego wysyłania dowolnych raportów do wybranych użytkowników poprzez mail.
55. System musi mieć możliwość automatycznego zapisywania raportów w formacie minimum: PDF, HTML i CSV.
56. Notyfikacje alertów muszą być wysyłane minimum poprzez mail.
57. System musi zapewniać funkcjonalność wznawiania zadań backupowych.

58. System musi zapewniać funkcjonalność równoległego wykonywania kopii danych backupowanych – inline copy (tego samego zestawu danych pojedynczego klienta) na minimum dwa docelowe urządzenia przechowywania danych.
59. 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.
60. Funkcjonalność multistreamingu musi być dostępna dla deduplikacji bez względu czy następuje na kliencie czy na serwerze systemu.
61. System musi zapewniać funkcjonalność multipleksowania kilku strumieni danych na nośniku taśmowym – tzw. multiplexing. Wydajny zapis wielu strumieni danych na taśmy bez pośrednictwa dysków.
62. Rozwiązanie musi posiadać możliwość wykonywania backupu pełnego, przyrostowego, różnicowego oraz syntetycznego.
63. System musi posiadać funkcję szyfrowania i kompresji danych transmitowanych przez LAN, możliwość wykorzystania szyfrowania i kompresji musi być dostępna w dowolnej kombinacji.
64. 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.
65. System musi posiadać (jako opcja) zintegrowane w systemie mechanizmy indeksowania pełnokontekstowego i wyszukiwania danych. Indeksowaniu powinny podlegać dane z backupowane i zarchiwizowane już znajdujące się w systemie.
66. System musi realizować funkcjonalność weryfikacji wykonanych kopii.
67. System powinien 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.
68. 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.
69. System musi umożliwiać odtwarzanie danych plikowych pomiędzy systemami operacyjnymi np. odtwarzanie danych plikowych Linux na systemie Windows.
70. Możliwość backupu i odtwarzania dedykowanym agentem dokumentów i maili dla Microsoft Office 365 z:
    - SharePoint Online;
    - Exchange Online;
    - OneDrive;
    - Teams;
    - ruch pocztowy SMTP.
71. Możliwość zwiększenia bezpieczeństwa systemu poprzez integrację z CyberArk (lub systemem równoważnym) 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.
72. Musi istnieć możliwość wskazania klucza szyfrującego (Bring Your Own Key – BYOK), który będzie wykorzystywany do szyfrowania kopii backupowych.
73. Automatyzacja – zarządzanie systemem poprzez API, Terraform, Ansible i PowerShell.

74. Workflow – dedykowany komponent do tworzenia i uruchamiania procesów obejmujących działania w obszarze backupu, odtwarzania oraz pozwalający na wykonywanie poleceń czy skryptów z systemów zewnętrznych.
75. 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.
76. Jako opcja 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 produkcyjnych.

Wymogi szczegółowe dla backupu maszyn wirtualnych

77. System musi wspierać backup całych maszyn wirtualnych/kontenerów dla czołowych rozwiązań wirtualizacyjnych, kontenerowych i chmurowych:
    - Alibaba Cloud;
    - Amazon;
    - Citrix Xen;
    - Google Cloud Platform;
    - Huawei FusionCompute;
    - Microsoft Azure;
    - Microsoft Azure Stack Hub;
    - Microsoft Azure Stack HCI;
    - Microsoft Hyper-V;
    - Kubernetes;
    - Nutanix Acropolis Hypervisor (AHV);
    - OpenStack;
    - Oracle Cloud Classic;
    - Oracle Cloud Infrastructure;
    - Oracle VM;
    - Red Hat OpenShift;
    - Red Hat Virtualization;
    - vCloud Director;
    - VMware.

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

78. 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 wymaganiach wirtualizatorów i być w cenie rozwiązania.
79. Przy odtwarzaniu danych środowisk kontenerowych musi istnieć możliwość selekcji zasobów podlegającym odtworzeniu.

80. 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.
81. System musi zapewniać automatyczne wykrywanie i dodawanie do polityki backupu nowych maszyn wirtualnych.
82. System musi umożliwiać odzyskanie i uruchomienie maszyn wirtualnych z kopii zapasowej bez oczekiwania na pełne przywrócenie maszyny wirtualnej minimum dla VMware i Hyper-V.
83. System musi umożliwiać konwertowanie maszyn wirtualnych pomiędzy wirtualizatorami, minimum:
    - VMware do: Hyper-V, Azure, Amazon, Google Cloud Platform, 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 z backupowanej maszyny wirtualnej istnieje możliwość wybrania innego wirtualizatora jako miejsca odtwarzania i uruchomienia odtworzonej maszyny wirtualnej.

84. System musi wspierać mechanizm CBT (change block tracking) minimum dla VMware i Hyper-V.
    - System musi umożliwiać konwersję z backupowanego serwera Windows i Linux do maszyny wirtualnej w środowiskach Hyper-V i VMware.
85. Możliwość (jako opcja) synchronizacji maszyn wirtualnych VMware do środowiska Amazon, Azure, Hyper-V, VMware celem budowy rozwiązania DR (Disaster Recovery) z funkcjonalnościami:
    - Failover (planowane i niezaplanowane/awaryjne);
    - Failback.
86. Jako opcja system 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.
87. System musi oferować integrację z mechanizmami deduplikacyjnymi urządzeń typu appliance (transfer danych bezpośrednio na urządzenia deduplikacyjne a tylko metadane wysyłane do systemu backupowego).
88. System musi oferować integrację z mechanizmami deduplikacyjnymi urządzeń typu appliance minimalne wsparcie to DDBoost i urządzenie StoreOnData Domain. Integracja z Data Domain 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).

Wymogi szczegółowe dla serwerów fizycznych

89. System musi wspierać backup (posiadać dedykowanego agenta backupowego) dla backupu zasobów plikowych, elementów systemu operacyjnego (np. System State dla systemów Windows) dla systemów operacyjnych klasy: Windows Server, Linux i Unix (minimum: AIX, Solaris, HP-UX).
90. System musi wspierać backup (posiadać dedykowanego agenta backupowego) dla backupu zasobów aplikacyjnych i bazodanowych (np. Oracle, SQL Server, SAP) dla systemów operacyjnych klasy: Windows Server, Linux i Unix (minimum: AIX, Solaris, HP-UX).
91. Musi być możliwość składowania kopii backupowej na lokalnym (zarządzanym przez serwer) zasobie: dysk wewnętrzny, udział sieciowy, napęd taśmowy, VTL czy storage obiektowy.
92. System musi pozwalać na zdalne i centralne zarządzanie komponentami backupowymi z konsoli administracyjnej o zakresie minimum:

- instalowanie agenta;
- modyfikacje komponentów (dodanie modułu, odinstalowanie modułu);
- pełne odinstalowanie agenta;
- monitorowanie logów backupowych z modułów backupowych;
- zarządzanie ustawieniami komunikacyjnymi dla agenta;
- restart komponentów;
- definiowanie właściciela serwera dla celów tzw.: private data a więc zabezpieczenia przed odtwarzaniem danych dla innych użytkowników.

Wymogi szczegółowe dla baz i aplikacji

93. Agent do spójnego backupu bazy HBASE – backup pełny i przyrostowy.
94. Agent do backupu systemów plikowych: Lustre, GlusterFS.
95. System musi umożliwiać wykonanie kopii na gorąco bazy danych MySQL, PostgreSQL, Oracle, Informix na dowolnej platformie systemu operacyjnego (Windows/Linux/Unix) poprzez dedykowanego agenta bazodanowego, transfer danych musi odbywać się bez pośredniczenia dysków, a więc transfer danych z agenta bazodanowego bezpośrednio do serwera backupowego celem zapisu na dany nośnik.
96. System musi umożliwiać wykonanie kopii na gorąco bazy danych SQL Server, Oracle, MySQL, PostgreSQL, DB2, Informix; konfiguracja agenta nie może powodować konieczności tworzenia skryptów uruchamianych po stronie klienta niezależnie czy jest to serwer fizyczny czy wirtualny. Brak skryptów musi dotyczyć dowolnych typów backupów: backup automatyczny uruchamiany poprzez harmonogram, backup manualny.
97. Odtwarzanie danych z backupu bazodanowego (SQL Server, Oracle, MySQL, PostgreSQL, DB2, Informix) musi odbywać się poprzez konsolę administracyjną bez konieczności konfigurowania skryptów.
98. Dla silników bazodanowych SQL Server, Oracle i SAP HANA, DB2 musi istnieć mechanizm backupu logów transakcyjnych z częstotliwością co 1 minutę nawet w przypadku, gdy serwer zarządzający systemem backupowym jest niedostępny.
99. Konfiguracja agentów backupowych dla: SQL Server, Oracle, MySQL, PostgreSQL musi odbywać się poprzez interfejs graficzny, jakakolwiek modyfikacja zasobów do backupu (np. dodanie nowej bazy) nie może powodować konieczności modyfikacji skryptów czy to dla backupów planowanych czy wykonywanych na żądanie.
100. System musi umożliwiać wykonanie kopii na gorąco Active Directory a następnie odzyskania pojedynczych obiektów AD wraz z hasłami użytkowników.
101. System musi umożliwiać odtwarzanie backupu wykonywanego online dedykowanym agentem, do pliku celem późniejszego odtwarzania bez udziały systemu. Funkcjonalność ta musi być dostępna minimum dla SQL Server, Oracle i Exchange.
102. System musi umożliwiać wykonanie kopii na gorąco aplikacji Microsoft Exchange a następnie odzyskania pojedynczych wiadomości. Dedykowany agent do backupu Exchange musi wspierać backup środowiska Exchange DAG poprzez nazwę DAG nawet w konfiguracji bez adresu IP.
103. System musi umożliwiać odtwarzanie pojedynczych tabel dla minimum: Oracle, DB2, PostgreSQL, MySQL, Informix, SQL Server.
104. Dla minimum MySQL i PostgreSQL musi istnieć mechanizm backupu z wykorzystaniem mechanizmu backupu blokowego.
105. Automatyczny backup logów transakcyjnych dla baz danych w oparciu o procent wolnego miejsca na systemie plikowym, minimum dla: Oracle, SQL, Notes, SAP/Oracle.
106. Dla SQL Server możliwość skonfigurowania rozszerzenia pozwalającego backupować i odtwarzać bazy bezpośrednio z konsoli Management Studio.

107. Wsparcie dla backupu online dla minimum Microsoft SQL Server 2005 / 2008 / 2008 R2 / 2012 / 2014 / 2016 / 2017 / 2019 / 2022 na platformie Windows.
108. Dedykowany agent bazodanowy dla backupu SQL Server (2017/2019/2022) na platformie Linux: Ubuntu, SuSe, RHEL.
109. Odtwarzanie baz SAP opartej na silniku Oracle do pliku, a więc odtwarzanie backupu online na dysk (tzw. application free restore).
110. Dedykowani agenci do backupu systemów Big Data: Hadoop, Greenplum, GPFS, Splunk, MongoDB.
111. Możliwość integracji kopii migawkowych dla backupu konsystentnego aplikacji i baz danych minimum: VMware, Hyper-V, SQL Server, Exchange, MySQL, Oracle – zarządzanie kopiami migawkowymi musi odbywać się z konsoli administracyjnej systemu backupowego a integracja zarządzania nie może odbywać się na bazie skryptów.
112. Jako opcja możliwość backupu danych z aplikacji Salesforce, minimalny zakres backupowanych danych to:
    - Standard objects;
    - Custom objects;
    - CRM content;
    - dokumenty;
    - załączniki;
    - pliki.
113. Jako opcja backup Active Directory i Microsoft Entra ID z możliwością backupu: Użytkowników, Grup, Conditional access policies, Enterprise applications, App registrations, Roles.

Wymogi dla licencjonowania (licencjonowanie typu perpertual)

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. Niedopuszczalne jest aby licencjonowanie zależne było od ilości serwerów fizycznych czy ich mocy (ilości procesorów) niezależnie czy dane są z nich backupowane bezpośrednio czy tworzą platformę wirtualizacyjną, która jest backupowana.
4. 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
5. Oferowana licencja oraz architektura systemu musi pozwalać na backup danych na:
    - nielimitowana ilość bibliotek taśmowych i napędów fizycznych;
    - nielimitowaną przestrzeń w rozwiązaniach chmurowych (minimum: AWS, Azure, Google).
6. W przypadku wielu lokalizacja licencja musi pozwalać na nielimitowaną replikację danych po deduplikacji pomiędzy lokalizacjami.
7. Zaoferowane licencje nie mogą mieć żadnych ograniczeń czasowych (muszą być wieczyste) dla wszystkich wymaganych funkcjonalności backupowych.
8. Zaoferowane oprogramowanie musi być licencjonowane per:
    - ilość maszyn wirtualnych podlegających backupowi niezależnie czy będą wykorzystywani agenci plikowi czy bazodanowi zainstalowani wewnątrz maszyny;
    - ilość aplikacji dla środowisk kontenerowych lub wielkość danych podlegającą backupowi;
    - ilość użytkowników dla backupu stacji roboczych;
    - ilość użytkowników aplikacji O365 lub Saleforce;

- ilość użytkowników Active Directory lub Microsoft Entra ID.

9. Do dostarczonych licencji jest wymagane 36 miesięczne wparcie producenta lub autoryzowanego partnera serwisowego (pierwsza i druga linia wsparcia świadczona w języku polskim lub angielskim) zapewniające wsparcie techniczne w trybie: poniedziałek – piątek, 7:00 – 19:00 oraz dostęp do bezpłatnych ewentualnych poprawek i uaktualnień.
10. Zaoferowane licencje na system muszą zapewnić backup danych z środowiska o wielkości:
    - środowisko maszyn wirtualnych (on premise i cloud) wraz z aplikacjami i bazami:
        i. ilość maszyn wirtualnych 120 sztuk;
    - środowisko serwerów fizycznych (w tym NAS) wraz z aplikacjami i bazami: 6 TB;
    - użytkowników Microsoft 365: 500;
11. Zaoferowane licencje muszą pozwalać na skanowanie antyransomware dla:
    - Danych plikowych o wielkości: 6 TB;
    - Maszyn wirtualnych w ilości: 120 sztuk.

3. **<u>Urządzenia dyskowe do przechowywania kopii zapasowych danych – 2 szt.</u>**
   - Urządzenie musi być przystosowane do montażu w szafie rack 19”.
   - Urządzenie musi oferować minimum 115TiB przestrzeni użytkowej dla danych (bez deduplikacji).
   - Dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID-6 zrealizowanej sprzętowo. Urządzenie musi weryfikować ewentualne przekłamanie danych w wyniku działań systemu plików / mechanizmów RAID zaimplementowanych w urządzeniu. Wymaga się, aby urządzenie sprawdzało sumy kontrolne zapisywanych fragmentów danych po przejściu danych przez system plików / mechanizmy RAID. Urządzenie musi automatycznie rozpoznawać i naprawiać błędy w locie. Urządzenie musi umożliwiać bezpieczne usuwanie danych zgodnie ze standardem NIST SP 800-88 poprzez mechanizm wielokrotnego nadpisania przeterminowanych danych. Jeżeli dla realizacji powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla nieograniczonej pojemności dostarczanego urządzenia.
   - Urządzenie musi umożliwiać rozbudowę pojemności użytkowej dla danych (bez deduplikacji) do co najmniej 180 TiB bez wliczania w to przestrzeni związanej z mechanizmami protekcji.
   - Urządzenie musi posiadać minimum: 2 porty FC 32 Gbps (Fibre Channel) wraz z odpowiednimi wkładkami oraz 2 porty z wkładkami optycznymi 25 Gbps SR możliwością obsługi protokołów CIFS i NFS na każdym z portów oraz deduplikacji na źródle oraz możliwość rozbudowy o kolejne 2 wkładki optyczne 10 lub 25 Gbps bez konieczności wymiany jakichkolwiek komponentów sprzętowych.
   - Urządzenie musi osiągać w maksymalnej konfiguracji wydajność backupu co najmniej 25 TB/godzinę z wykorzystaniem deduplikacji na źródle (wg danych podawanych przez producenta). Urządzenie nie może zmniejszać swojej wydajności w czasie przybywania kolejnych danych. Urządzenie musi pozwalać na jednoczesną obsługę minimum 250 strumieni (zapis danych, odczyt danych, replikacja danych).
   - Urządzenie musi umożliwiać jednoczesny dostęp do całej pojemności urządzenia wszystkimi poniższymi protokołami: CIFS, NFS i deduplikacja na źródle (OST/Boost/Catalyst) dla interfejsów 10/25 Gbps, VTL i deduplikacja na źródle (OST/BOOST/CATALYST) dla interfejsów FC. Urządzenie musi posiadać obsługę mechanizmów deduplikacji dla danych otrzymywanych wszystkimi protokołami (CIFS, NFS, VTL, deduplikacja na źródle) przechowywanych w obrębie urządzenia. Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych LTO oraz emulacji bibliotek taśmowych. Urządzenie musi umożliwiać przyporządkowanie minimum 4096 slotów do pojedynczej biblioteki taśmowej. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
   - Urządzenie musi umożliwiać podział na minimum 36 partycje logiczne w taki sposób, aby każdy z podłączonych systemów backupowych mógł pracować na osobnym urządzeniu logicznym. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
   - Urządzenie musi deduplikować dane inline przed zapisem na nośnik dyskowy. Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych. Oznacza to, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości. Proces deduplikacji musi odbywać się inline – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z dodatkowego bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej). Wszystkie unikalne, zdeduplikowane bloki przed zapisaniem na dysk muszą być kompresowane. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
   - Urządzenie musi umożliwiać replikację danych do drugiego urządzenia. Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane muszą być tylko te fragmenty danych (bloki), które nie znajdują się na docelowym urządzeniu. W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie

strumienia replikacji tymi samymi portami. Musi istnieć możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami. Zarządzanie całym procesem kopiowania danych oraz wszystkimi kopiami musi być możliwy z poziomu oprogramowania backupowego. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.

- Urządzenie musi mieć zaimplementowaną funkcjonalność wewnętrznego mechanizmu szyfrowania danych AES-256 realizowaną na poziomie urządzenia zgodnie ze standardem FIPS 140-2. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej pojemności urządzenia.
- Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nienależące do backupów o aktualnej retencji) w procesie czyszczenia. Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu i odtwarzania danych. Musi istnieć możliwość zdefiniowania czasu, w którym wykonywany jest proces usuwania przeterminowanych danych (czyszczenia).
- Urządzenie musi mieć możliwość zarządzania poprzez interfejs graficzny dostępny z przeglądarki internetowej. Oprogramowanie do zarządzania musi rezydować oferowanym na urządzeniu deduplikacyjnym. Urządzenie musi umożliwiać ustawienie powiadomień administratora o problemach w urządzeniu za pomocą poczty elektronicznej.
- Urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia) co najmniej następujące aplikacje backupujące bezpośrednio na oferowane urządzenie: Dell EMC Networker, Micro Focus Data Protector, IBM BRMS, IBM Spectrum Protect, Veeam, Veritas NetBackup, Commvault, Microsoft SQL Server, Oracle RMAN, SAP i SAP HANA. W przypadku przyjmowania backupów od aplikacji: Micro Focus Data Protector, Veeam, Veritas NetBackup, Commvault, Microsoft SQL Server, Oracle RMAN, SAP/Oracle i SAP HANA urządzenie musi umożliwiać deduplikację na źródle i przesłanie tylko nowych, unikalnych bloków danych poprzez sieć FC i Ethernet.
- Urządzenie musi być wyposażone w zasilacze i wentylatory redundantne, tzn. awaria pojedynczego urządzenia nie wpływała na stabilną pracę całego urządzenia.
- Urządzenie musi być kompletnym rozwiązaniem sprzętowym typu „appliance” pochodzącym od jednego producenta. Nie dopuszcza się rozwiązania zbudowanego z niezależnych komponentów sprzętowo-programowych. Urządzenie powinno być oficjalnie dostępne w ofercie producenta przed ukazaniem się niniejszego postepowania.
- 3-letnia gwarancja producenta w miejscu instalacji z czasem reakcji w ciągu następnego dnia roboczego. W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z urządzeniem oraz oprogramowania wewnętrznego urządzenia. Gwarancja na sprzęt musi być dostarczona i realizowana przez organizację serwisową producenta sprzętu. Producent sprzętu musi posiadać certyfikat ISO 9001:2015 dla przedstawicielstwa w Polsce na sprzedaż oraz serwis urządzeń storage. Serwis musi być realizowany przez producenta sprzętu w języku polskim.
- Urządzenia muszą być nowe i zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta oraz deklaracje zgodności CE.

4. **Serwer skanowania kopii zapasowych – 1 szt.**
   - Maksymalnie 1U RACK 19 cali wraz z szynami montażowymi i ramieniem kablowym umożliwiającym wysunięcie, do celów serwisowych, serwera z szafy bez konieczności odłączania kabli zasilających i sygnałowych (kable LAN SAN). Serwer wyposażony w zdejmowany panel przedni. Możliwość wyposażenia w zamknięcie panelu na klucz. Serwer wyposażony w fabryczny moduł TPM 2.0. Jako opcja możliwość instalacji czujnika otwarcia obudowy współpracującego z BIOS/UEFI.
   - Procesor 16-rdzeniowy, x86 - 64 bity, AMD EPYC 9124 (3.0GHz/16-core/200W) lub równoważny procesor 16-rdzeniowy, osiągający w testach SPECrate2017_int_base powyżej 173 punktów wraz z oferowanym serwerem. W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie www.spec.org. Płyta główna wspierająca zastosowanie procesorów od 16 do 128-rdzeniowych, mocy do min. 400W i taktowaniu CPU do min. 4.1GHz.
   - Min. 1 procesor, płyta główna min. jednoprocesorowa.
   - Pamięć operacyjna 16GB RDIMM DDR5 min. 4800 MT/s w modułach o pojemności min. 16GB. Płyta główna z minimum 12 slotami na pamięć i umożliwiająca instalację minimum 3TB. Obsługa zabezpieczeń: Advanced ECC.
   - Serwer musi być wyposażony w: 1 aktywne gniazdo PCI Express generacji 5, gniazdo x16, możliwość rozbudowy do 2 gniazd PCI Express generacji 5, serwer musi mieć dodatkowo dedykowane dwa sloty OCP: na kontroler dyskowy lub na kartę sieciową niezajmującą slotów PCI-Express.
   - Zatoki dyskowe gotowe do zainstalowania min.8 dysków 2.5” typu Hot-Swap, NVME/SAS12G/SATA/SSD. Zainstalowane: 2 dyski 480GB SATA6G SSD Read-Intensive.
   - Serwer wyposażony w kontroler sprzętowy, zapewniający obsługę 16 napędów dyskowych NVMe/SAS12G oraz obsługujący poziomy: RAID 0/1/10. Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie.
   - Minimum 2 porty Ethernet 10/25GbE SFP+ które nie zajmują gniazd PCI Express opisanych w sekcji „Sloty rozszerzeń” z chipsetem BCM 57414 oraz dostarczona z wkładkami 25GB SR.
   - Zintegrowana karta graficzna.
   - Porty 5 x USB 3.2 Gen1 (w tym min. 2 porty wewnętrzne), 1x VGA, Możliwość rozbudowy/rekonfiguracji o: port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45 oraz bez konieczności instalowania kart w slotach PCI-Express.
   - Zasilacz 2 szt., typu Hot-Plug, redundantne, każdy o mocy minimum 1000W.
   - Zestaw wentylatorów redundantnych typu Hot-Plug.
   - Karta/moduł zarządzający: niezależna od systemu operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCI Express w serwerze, posiadająca minimalną funkcjonalność:
     - monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne);
     - wsparcie dla pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP;
     - dostęp do karty zarządzającej poprzez dedykowany port RJ45 z tyłu serwera lub przez współdzielony port zintegrowanej karty sieciowej serwera;
     - dostęp do karty możliwy:
       - z poziomu przeglądarki webowej (GUI),
       - z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP),
       - poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface);
     - wbudowane narzędzia diagnostyczne;
     - zdalna konfiguracji serwera(BIOS) i instalacji systemu operacyjnego;
     - obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie;
     - wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników;
     - przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough);

- obsługa zdalnego serwera logowania (remote syslog);
- wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów CD/DVD i USB i wirtualnych folderów;
- mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie;
- funkcja zdalnej konsoli szeregowej przez SSH (wirtualny port szeregowy);
- monitorowanie zasilania oraz zużycia energii przez serwer w czasie z możliwością graficznej prezentacji;
- konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping);
- zdalna aktualizacja oprogramowania (firmware);
- zarządzanie grupami serwerów, w tym:
  - tworzenie i konfiguracja grup serwerów,
  - sterowanie zasilaniem (wł/wył),
  - ograniczenie poboru mocy dla grupy (power caping),
  - aktualizacja oprogramowania (firmware),
  - wspólne wirtualne media dla grupy;
- możliwość równoczesnej obsługi przez min. 2 administratorów;
- autentykacja dwuskładnikowa (Kerberos);
- wsparcie dla Microsoft Active Directory;
- obsługa TLS i SSH;
- wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API;
- możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP).

- Wraz z serwerem należy dostarczyć system operacyjny Windows Serwer 2025 Standard (lub Datacenter) na wszystkie fizyczne rdzenie w zainstalowanym procesorze dopuszcza się licencje OEM oraz ROK lub równoważny system operacyjny.
- 3-letnia gwarancja i serwis producenta w miejscu instalacji z czasem reakcji w ciągu następnego dnia roboczego od zgłoszenia. Zgłoszenia przyjmowane w trybie 24x7. W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania wewnętrznego urządzenia. Gwarancja na sprzęt musi być dostarczona i realizowana przez organizację serwisową producenta sprzętu. Producent sprzętu musi posiadać certyfikat ISO 9001:2015 dla przedstawicielstwa w Polsce na sprzedaż oraz serwis urządzeń. Serwis musi być realizowany przez producenta sprzętu w języku polskim.
- Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta oraz deklaracje zgodności CE.

5. **Serwery zarządzania i przesyłania danych – 2 szt.**
   - Maksymalnie 2U RACK 19 cali wraz z szynami montażowymi i ramieniem kablowym umożliwiającym wysunięcie, do celów serwisowych, serwera z szafy bez konieczności odłączania kabli zasilających i sygnałowych (kable LAN SAN). Serwer wyposażony w zdejmowany panel przedni. Możliwość wyposażenia przedniego panelu w zamknięcie. Serwer wyposażony w TPM 2.0. Jako opcja możliwość instalacji czujnika otwarcia obudowy współpracującego z BIOS/UEFI/kartą zdalnego zarządzania.
   - procesor 24-rdzeniowy, x86 - 64 bity, AMD EPYC 9224 (2.5GHz/24-core/200W) lub równoważny procesor 24-rdzeniowy, osiągający w testach SPECrate2017_int_base powyżej 500 punktów w konfiguracji dwuprocesorowej. W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie www.spec.org. Płyta główna wspierająca zastosowanie procesorów od 16 do 128-rdzeniowych, mocy do min. 400W i taktowaniu CPU do min. 4.1GHz.
   - Min. 1 procesor z możliwością rozbudowy do 2 procesorów.
   - Pamięć operacyjna 128GB RDIMM DDR5 min. 4800 MT/s w modułach o pojemności min. 32GB każdy. Płyta główna z minimum 24 slotami na pamięć i umożliwiająca instalację minimum 6TB. Obsługa zabezpieczeń: Advanced ECC.
   - Min. 3 aktywne gniazda min. PCI Express generacji 5, pełnej wysokości (full height), w tym min. 3 slot x16 (szybkość slotu – bus width). Możliwość rozbudowy/rekonfiguracji do min. 6 slotów PCI Express generacji 5 pełnej wysokości (full height).
   - Zatoki dyskowe gotowe do zainstalowania min. 8 dysków 2.5" typu Hot-Swap, NVMe/SAS/SATA/SSD. Możliwość rozbudowy/rekonfiguracji serwera do min. 16 dysków 2,5". Wszystkie zatoki dyskowe dostępne z przodu serwera. Zainstalowane: 2 dyski 3,2TB NVMe Mix-Use SSD.
   - Serwer wyposażony w kontroler sprzętowy z min. 4GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę 8 napędów dyskowych NVMe/SAS oraz obsługujący poziomy: RAID 0/1/10/5/50/6/60. Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie.
   - Minimum 1 karta 10/25Gb SFP28 zapewniająca min. 2 porty, wszystkie porty obsadzone wkładkami SFP28 25Gb SR, karta z chipsetem BCM57414, karta nie zajmuje slotów opisanych w punkcie „Sloty rozszerzeń".
   - Minimum 2 porty FC 32Gb każdy, każdy port z wkładką FC 32Gb SW.
   - Zintegrowana karta graficzna.
   - 5 portów USB 3.2 Gen1 (w tym min. 2 porty wewnętrzne), 1x VGA, Możliwość rozbudowy/rekonfiguracji o port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45 oraz bez konieczności instalowania kart w slotach PCI Express.
   - Zasilacz 2 szt., typu Hot-Plug, redundantne, każdy o mocy minimum 1000W.
   - Zestaw wentylatorów redundantnych typu Hot-Plug.
   - Karta/moduł zarządzający: niezależna od systemu operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność:
     - monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski (fizyczne i logiczne);
     - wsparcie dla pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP;
     - dostęp do karty zarządzającej poprzez dedykowany port RJ45 z tyłu serwera lub przez współdzielony port zintegrowanej karty sieciowej serwera;
     - dostęp do karty możliwy:
       - z poziomu przeglądarki webowej (GUI),
       - z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP),

  - poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface);
- wbudowane narzędzia diagnostyczne;
- zdalna konfiguracji serwera(BIOS) i instalacji systemu operacyjnego;
- obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie;
- wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników;
- przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough);
- obsługa zdalnego serwera logowania (remote syslog);
- wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów CD/DVD i USB i wirtualnych folderów;
- mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie;
- funkcja zdalnej konsoli szeregowej przez SSH (wirtualny port szeregowy);
- monitorowanie zasilania oraz zużycia energii przez serwer w czasie z możliwością graficznej prezentacji;
- konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping);
- zdalna aktualizacja oprogramowania (firmware);
- zarządzanie grupami serwerów, w tym:
  - tworzenie i konfiguracja grup serwerów,
  - sterowanie zasilaniem (wł/wył),
  - ograniczenie poboru mocy dla grupy (power caping),
  - aktualizacja oprogramowania (firmware),
  - wspólne wirtualne media dla grupy;
- możliwość równoczesnej obsługi przez min. 2 administratorów;
- autentykacja dwuskładnikowa (Kerberos);
- wsparcie dla Microsoft Active Directory;
- obsługa TLS i SSH;
- wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API;
- możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP).

- Wraz z serwerem należy dostarczyć system operacyjny Windows Serwer 2025 Standard (lub Datacenter) na wszystkie fizyczne rdzenie w zainstalowanym procesorze dopuszcza się licencje OEM oraz ROK lub równoważny system operacyjny.
- 3-letnia gwarancja i serwis producenta w miejscu instalacji z czasem reakcji w ciągu następnego dnia roboczego od zgłoszenia. Zgłoszenia przyjmowane w trybie 24x7. W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania wewnętrznego urządzenia. Gwarancja na sprzęt musi być dostarczona i realizowana przez organizację serwisową producenta sprzętu. Producent sprzętu musi posiadać certyfikat ISO 9001:2015 dla przedstawicielstwa w Polsce na sprzedaż oraz serwis urządzeń. Serwis musi być realizowany przez producenta sprzętu w języku polskim.
- Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta oraz deklaracje zgodności CE.

6. **<u>Dodatkowe wymagania dotyczące całości systemu:</u>**
   - Wykonawca zapewni obsługę gwarancyjną sprzętu oraz oprogramowania na okres nie krótszy niż 3 lata licząc od daty dokonania odbioru końcowego bez zastrzeżeń – dopuszczalne jest, że w ramach tej gwarancji wykonawca wykupi na własny koszt usługi serwisowe u producenta rozwiązania.
   - Wszystkie urządzenia zgodne z zasilaniem zewnętrznym 230V ±10%, 50Hz.
7. **<u>W ramach oferty należy uwzględnić:</u>**
   - Wdrożenie rozwiązania w zakresie:
     - opracowanie projektu technicznego;
     - dostawa urządzenia do wskazanej lokalizacji;
     - instalacja urządzeń w szafie rack;
     - okablowanie i oznakowanie przewodów;
     - inicjalizacja urządzeń, aktualizacja oprogramowania układowego;
     - konfiguracja zasobów urządzenia dyskowego kopii zapasowych zgodnie z projektem;
     - rekonfiguracja zoningu na przełącznikach SAN;
     - przygotowanie OS oraz instalacja i konfiguracja serwerów backup;
     - przygotowanie OS oraz instalacja i konfiguracja serwera skanowania kopii zapasowych;
     - instalacja i konfiguracja Proxy w oddziałach na maszynach wirtualnych;
     - konfiguracja polityk backupowych do centrali i oddziałów;
     - konfiguracja synchronizacji oraz replikacji danych;
     - nadzór nad wykonaniem pierwszej kopii zapasowej;
     - test poprawności odtwarzania dla 1 VM lokalnej i 1 VM z każdego oddziału;
     - test poprawności odtwarzania z serwerów NAS dla pojedynczych plików;
     - zdalne wsparcie powdrożeniowe w zakresie 30 godzin;
     - dokumentacja powykonawcza.
   - Przeszkolenie z zakresu maszyn wirtualnych i fizycznych – w wymiarze 4h.
   - Przeszkolenie z zakresu procesu weryfikacji kopii i odzyskiwania systemu – w wymiarze 4h.
   - Wsparcie powdrożeniowe przez okres 12 miesięcy – w wymiarze 30h.