Ministerstwo
Edukacji i Nauki

Biuro Dyrektora Generalnego

BDG-WII.072.3.2023

Warszawa, dnia 6 kwietnia 2023 r.

Wykonawcy

ZAPYTANIE O WYCENĘ

Ministerstwo Edukacji i Nauki (MEiN), ul. Wspólna 1/3, 00-529 Warszawa (NIP 7011010460, REGON 387796051) zwraca się z prośbą o przedstawienie propozycji cenowej (oszacowanie wartości zamówienia) dotyczącej zakupu **rozbudowy Centralnego Systemu Kopii Zapasowych wraz z appliance oraz 3 letnim wsparciem producenta**.

Opis przedmiotu zamówienia został określony w *Załączniku nr 1* do zapytania o wycenę.

Wycenę, sporządzoną na Formularzu będącym *Załącznikiem nr 2* do zapytania o wycenę, proszę przesłać na adres oferty@mein.gov.pl **do dnia 14 kwietnia 2023 r., godz. 12:00** (w tytule wiadomości proszę wpisać: „WYCENA – sprawa: BDG-WII.072.3.2023)".

Ewentualne pytania mające wpływ na przedmiotową wycenę proszę kierować na adres mailowy jak wyżej.

Załączniki:

1) Opis przedmiotu zamówienia
2) Formularz wyceny

Łukasz Tererycz
Zastępca Dyrektora
/ – podpisano cyfrowo/

tel. (22) 52 92 725, (22) 34 74 157
sekretariat.bdg@mein.gov.pl, sekretariat.bdg.edukacja@mein.gov.pl
www.mein.gov.pl

ul. Wspólna 1/3
00-529 Warszawa

Załącznik nr 1 do zapytania o wycenę

OPIS PRZEDMIOTU ZAMÓWIENIA

Rozbudowa Centralnego Systemu Kopii Zapasowych wraz z appliance oraz 3-letnim wsparciem producenta.

Zamawiający posiada aktualnie:

Ilość licencji	Nazwa licencji
7	NETBACKUP PLATFORM BASE COMPLETE ED WITH FLEXIBLE LICENSING XPLAT 1 FRONT END TB PLUS ONPREMISE STANDARD PERPETUAL LICENSE GOV
4	NETBACKUP PLATFORM BASE COMPLETE ED WITH FLEXIBLE LICENSING XPLAT 1 FRONT END TB PLUS ONPREMISE STANDARD PERPETUAL LICENSE CORPORATE
3	NETBACKUP PLATFORM BASE COMPLETE ED XPLAT 1 FRONT END TB ONPREMISE STANDARD PERPETUAL LICENSE CORPORATE

Przedmiotem zamówienia jest odnowienie wsparcia dla obecnie posiadanych licencji oraz powiększenie możliwej do backupowania przestrzeni o kolejne 14 TB wraz z 3-letnim wsparciem producenta.

Łącznie System Kopii Zapasowych musi licencyjnie zabezpieczyć 28 TB danych Zamawiającego nie wliczając danych zdeduplikowanych i skompresowanych.

Dodatkowo System Kopii zapasowych musi być rozbudowany o fizyczny appliance o pojemności 75 TB wraz z niezbędnymi licencjami i 3-letnim wsparciem producenta.

Wszystkie elementy systemów muszą pochodzić od jednego producenta z legalnego kanału sprzedaży na terenie Unii Europejskiej.

System musi składać się z następujących elementów:

1. System kopii zapasowych

Lp.	MINIMALNE WYMAGANIA ZAMAWIAJĄCEGO
1.	Oprogramowanie systemu powinno być przeznaczone dla średnich i dużych firm, posiadających rozbudowane środowisko informatyczne.
2.	W celu zapewnienia dużej elastyczności i skalowalności środowiska kopii zapasowych oprogramowanie systemu powinno posiadać trójwarstwową architekturę: Serwer Zarządzający, Serwer Mediów, Klient.
3.	Oprogramowanie systemu powinno umożliwiać wykonywanie kopii zapasowych w środowisku heterogenicznym za pomocą, dedykowanego dla platformy systemowej, klienta systemu kopii zapasowych.
4.	System powinien umożliwiać łatwą rozbudowę w miarę rozrastania się infrastruktury informatycznej Zamawiającego, poprzez dokładanie kolejnych centralnie zarządzanych Serwerów Mediów.
5.	Proponowane rozwiązanie musi umożliwiać uruchomienie serwera zarządzającego kopiami zapasowymi na głównych platformach Windows, Linux i Unix.
6.	Proponowane rozwiązanie musi wspierać wysoką dostępność (klastrowanie) serwera kontrolującego kopie zapasowe
7.	Oprogramowanie musi być niezależne pod względem sprzętowym i nie może preferować instalacji na platformie sprzętowej jednego producenta. Powinno

	udostępniać te same funkcjonalności niezależnie od tego na jakiej platformie systemowej będzie zainstalowane. Zamawiający musi posiadać możliwość zmiany platformy sprzętowej bez utraty funkcjonalności systemu kopii zapasowej.
8.	Proponowane rozwiązanie musi wspierać wdrożenia na sprzęcie fizycznym, infrastrukturze wirtualnej oraz w chmurze.
9.	Proponowane rozwiązanie musi umożliwiać administrację za pomocą GUI (aplikacja lub web), CLI oraz RESTful API
10.	System powinien posiadać centralną konsolę zarządzania środowiskiem kopii zapasowych. Konsola musi umożliwiać: ✓ monitorowanie i zarządzanie wszystkimi zadaniami wykonywania i odtwarzania kopii zapasowych, tworzenia duplikatów wykonanych kopii zapasowych, ✓ ustawianie harmonogramów wykonywania kopii zapasowych, ✓ monitorowanie i kontrolowanie urządzeń składowania kopii zapasowych podłączonych do Serwerów Mediów, ✓ centralne zarządzanie konfiguracją, właściwych dla oprogramowania systemu, ustawień Serwera Zarządzającego, Serwera Mediów, Klientów, ✓ uruchomienie odtwarzania kopii zapasowych na kliencie,
11.	Oprogramowanie systemu musi posiadać obsługę z poziomu wiersza poleceń w systemach Linux, Unix i Windows. Obsługa z poziomu wiersza poleceń musi umożliwiać: ✓ konfigurację i modyfikację polityk wykonywania kopii zapasowych, ✓ konfigurację i modyfikację harmonogramów wykonywania kopii zapasowych, ✓ konfigurację i modyfikację urządzeń składowania kopii zapasowych podłączonych do Serwerów Mediów, ✓ konfigurację i modyfikację nośników taśmowych, ✓ monitorowanie i kontrolowanie zadań kopii zapasowych, ✓ konfigurację i modyfikację nośników taśmowych ✓ konfigurację i modyfikację właściwych dla oprogramowania systemu, ustawień Serwera Zarządzającego, Serwera Mediów, Klientów, ✓ konfigurację, modyfikację i przeglądanie dzienników Serwera Zarządzającego, Serwera Mediów, Klientów,
12.	Rozwiązanie powinno być dostępne także jako zintegrowane programowo i sprzętowo urządzenie (appliance), a więc sprzęt i oprogramowanie backupowe razem. Zintegrowane urządzenia powinny umożliwiać zbudowanie w pełni funkcjonującej trzywarstwowej architektury backupowej z funkcjonalnością deduplikacji danych.
13.	Baza katalogowa dla systemu backupowego musi być częścią systemu backupowego i wspierać platformy minimum Linux, Windows oraz Unix oraz nie powinna posiadać ograniczeń wynikających z ilości używanych w serwerze procesorów i rdzeni procesorów.
14.	Baza katalogowa musi być w cenie systemu kopii zapasowych i nie ograniczona co do ilości środowisk backupowych, mocy czy ilości serwerów czy to backupowych czy produkcyjnych. Jakakolwiek rozbudowa środowiska backupowego czy dodanie następnego nie może powodować konieczności dokupienia licencji dla tej bazy.
15.	Oprogramowanie systemu kopii zapasowych musi posiadać zintegrowane zarządzanie kluczami szyfrującymi oraz musi posiadać możliwość integracji z zewnętrznymi usługami zarządzania kluczami szyfrowania.

16.	Oprogramowanie systemu kopii zapasowych musi integrować się z urządzeniami dyskowymi (deduplikatory) wspierającymi mechanizm WORM w celu ochrony danych przed zaszyfrowaniem, modyfikacją i usunięciem. Funkcjonalność musi zapewniać, że obraz kopii zapasowej jest tylko do odczytu i nie może być modyfikowany, uszkodzony lub zaszyfrowany po utworzeniu kopii zapasowej oraz chronić obraz kopii zapasowej przed usunięciem przed upływem terminu ważności.
17.	Obsługa funkcjonalności WORM powinna być realizowana natywnie przez oprogramowanie kopii zapasowych, gdzie zarządzanie czasem ochrony przechowywanych na urządzeniu obrazów kopii zapasowych odbywa się z poziomu oprogramowania systemu backupu, a nie rozdzielnie
18.	Proponowane rozwiązanie musi wspierać ochronę klientów pracujących pod kontrolą: ✓ Canonical Ubuntu w wersji 16 i nowszej ✓ CentOS 6.8 i nowsze ✓ Debian 7 - 10 ✓ IBM AIX 6.1 - 7.2 na architekturze IBM Power ✓ Windows 7 - 10 ✓ Windows Server 2008 - 2019, w tym wydania półroczne ✓ Oracle Linux 6.8 i nowsze ✓ Oracle Solaris 10 Update 11 i nowsze na architekturach Sparc i x64 ✓ Red Hat Enterprise Linux 6.8 i nowsze dla architektury x64 ✓ Red Hat Enterprise Linux 7.2 i nowsze dla architektury x64 ✓ Red Hat Enterprise Linux 7.2 i nowsze dla architektury IBM Power ✓ Red Hat Enterprise Linux 6.8 i 7.x na IBM System Z ✓ SUSE Enterprise Server 12 SP2 i nowsze na architekturach x64, IBM Power i IBM System Z
19.	Proponowane rozwiązanie musi wspierać architekturę składowania kopii zapasowych D2D2T i D2D2C.
20.	Proponowane rozwiązanie musi obsługiwać dowolny typ pamięci dyskowej (DAS, NAS, SAN) dla repozytorium backupu.
21.	Proponowane rozwiązanie musi wspierać storage taśmowy (samodzielne napędy taśmowe oraz biblioteki taśmowe w tym m.in. biblioteki robotów sterowane ACS) głównych producentów.
22.	Proponowane rozwiązanie musi deduplikować dane na źródle i celu.
23.	Deduplikacja musi umożliwiać wybór pomiędzy zmiennym i stałym rozmiarem bloku. Rozmiar bloku musi umożliwiać jego wybór.
24.	Proponowane rozwiązanie musi wspierać deduplikację zarówno inline jak i postprocesową.
25.	Proponowane rozwiązanie musi wspierać urządzenia deduplikacyjne głównych producentów takich jak Dell EMC, Exagrid, HPE, Quantum, NEC
26.	Proponowane rozwiązanie musi obsługiwać wirtualne biblioteki taśmowe (VTL)
27.	Proponowane rozwiązanie musi wspierać transfer danych zarówno przez sieć LAN jak i SAN.
28.	Proponowane rozwiązanie musi wspierać głównych dostawców chmur publicznych jako magazyn kopii zapasowych.

29.	Proponowane rozwiązanie musi obsługiwać deduplikację do chmury w celu minimalizacji transferu danych.
30.	Proponowane rozwiązanie musi umożliwiać wznowienie nieudanego zadania backupowego od ostatniego punktu kontrolnego.
31.	Proponowane rozwiązanie musi automatyzować tworzenie wielu kopii zapasowych na różnych urządzeniach magazynowych z różną długością przechowywania danych.
32.	Proponowane rozwiązanie powinno posiadać możliwość wykonywania wysokowydajnych kopii zapasowych serwerów z bardzo obciążonymi systemami plików na dyskach z dużą liczbą plików (np. backup typu disk-image)
33.	Proponowane rozwiązanie musi zapewniać możliwość wykonywania backupu syntetycznego.
34.	Proponowane rozwiązanie musi umożliwiać tworzenie ręcznych kopii zapasowych ad-hoc.
35.	Proponowane rozwiązanie musi wspierać topologie replikacji danych typu jeden-do-jednego, wiele-do-jednego, jeden-do-wielu oraz kaskadową z wykorzystaniem deduplikacji danych w celu zminimalizowania ilości przesyłanych danych.
36.	Proponowane rozwiązanie musi wspierać szyfrowanie danych.
37.	Proponowane rozwiązanie musi umożliwiać wznowienie nieudanego zadania przywracania z ostatniego punktu kontrolnego.
38.	Proponowane rozwiązanie musi zapewniać funkcje umożliwiające natywne odzyskiwanie "bare metal" (w pełni zautomatyzowane odzyskiwanie obejmujące system operacyjny, konfigurację, aplikacje i dane) klientów Windows, Linux, Solaris, AIX i HPUX bez konieczności korzystania z zewnętrznych/rodzimych narzędzi do odzyskiwania/reimaging systemu operacyjnego.
39.	Proponowane rozwiązanie musi umożliwiać przywracanie różnych konfiguracji systemu oraz różnych układów dysków.
40.	Proponowane rozwiązanie musi zapewniać możliwość konwersji P2V i V2P
41.	Proponowane rozwiązanie musi umożliwiać przywracanie nawet po wygaśnięciu wsparcia technicznego oprogramowania.
42.	Proponowane rozwiązanie musi umożliwiać przywracanie pojedynczych obiektów Active Directory z kopii zapasowej Windows System State
43.	Rozwiązanie musi wspierać VMware: ✓ Proponowane rozwiązanie musi wspierać VMware vSphere 6.0 i nowsze ✓ Proponowane rozwiązanie musi wspierać serwery vSphere zarządzane przez vCenter jak i samodzielne serwery ESXi ✓ Proponowane rozwiązanie musi wspierać VMware vSAN 6.5 i nowsze ✓ Proponowane rozwiązanie musi wspierać VMware vCloud Director 9.x ✓ Proponowane rozwiązanie musi wspierać wszystkie tryby transportu danych obsługiwane przez VDDK 6.7.2 (SAN, NBD, NBDSSL, hot-add) ✓ Proponowane rozwiązanie nie może wymagać instalacji agentów w maszynach wirtualnych w celu wykonywania kopii zapasowych ✓ Proponowane rozwiązanie musi wspierać śledzenie zmian (CBT - change block tracking)

	✓ Proponowane rozwiązanie musi wspierać tworzenie syntetycznych kopii zapasowych (tworzonych na podstawie ostatniego pełnego backupu oraz backupu przyrostowego CBT) maszyn wirtualnych VMware w celu umożliwienia wykonywania backupów przyrostowych (incremental-forever) ✓ Proponowane rozwiązanie musi zawierać mechanizm automatycznego wykrywania i ochrony maszyn wirtualnych VMware bez konieczności zmiany polityk backupu ✓ Proponowane rozwiązanie musi umożliwiać wyłączenie z backupu maszyn wirtualnych, usuniętych bloków oraz pliku swap ✓ Proponowane rozwiązanie musi wspierać przywracanie pojedynczego pliku z kopii zapasowej maszyny wirtualnej VMware bez konieczności uruchamiania agenta w maszynie wirtualnej oraz umieszczania wirtualnego dysku wirtualnego dysku w tymczasowej lokalizacji, jeżeli obraz kopii zapasowej jest przechowywany na taśmach ✓ Proponowane rozwiązanie musi wspierać jednoprzebiegowy backup Microsoft Exchange, Microsoft SQL Server oraz Microsoft SharePoint z możliwością przywracania elementów granularnych zgodnie z opisem w dalszej części. ✓ Proponowane rozwiązanie nie może wymagać wykonywania osobnego backupu na poziomie aplikacji lub wysyłki logów w przypadku backupu Microsoft Exchange, Microsoft SQL Server i Microsoft SharePoint ✓ Proponowane rozwiązanie musi wspierać limitowanie zasobów takich jak liczba jednoczesnych zadań backupu na serwer ESXi, klaster lub magazyn danych ✓ Proponowane rozwiązanie musi umożliwiać uruchomienie maszyny wirtualnej bezpośrednio z dyskowego repozytorium kopii zapasowych ✓ Proponowane rozwiązanie musi zapewniać natychmiastowy dostęp do chronionych maszyn wirtualnych i ich plików ✓ Proponowane rozwiązanie musi zapewniać dodatkowe możliwości administracji, monitorowania i odzyskiwania danych poprzez VMware vCenter Web Client
44.	Rozwiązanie musi wspierać Microsoft Hyper-V: ✓ Proponowane rozwiązanie musi wspierać Microsoft Hyper-V 2008 SP2 i nowsze ✓ Proponowane rozwiązanie musi wykorzystywać Windows Management Instrumentation (WMI) dla ochrony maszyn wirtualnych działających na platformie Hyper-V 2016 i nowszych ✓ Proponowane rozwiązanie musi wspierać ochronę maszyn wirtualnych rezydujących na systemach plików NTFS, ReFS, Windows Storage Spaces, Storage Spaces Direct oraz SMB 3.0 ✓ Proponowane rozwiązanie musi wspierać Resilient Change Tracking (RCT) ✓ Proponowane rozwiązanie musi wspierać tworzenie syntetycznych kopii zapasowych (tworzonych na podstawie ostatniego pełnego i przyrostowego backupu RCT) maszyn wirtualnych Hyper-V w celu umożliwienia tworzenia kopii zapasowych przyrostowych na zawsze ✓ Proponowane rozwiązanie musi wspierać ograniczenie liczby aktywnych snapshotów lub backupów na serwer Hyper-V i klaster

	✓ Proponowane rozwiązanie musi zawierać mechanizm automatycznego wykrywania i ochrony maszyn wirtualnych Hyper-V VM bez konieczności zmiany polityk backupu. ✓ Proponowane rozwiązanie musi umożliwiać wykluczenie usuniętych bloków i plików swap z kopii zapasowej maszyny wirtualnej Hyper-V ✓ Proponowane rozwiązanie musi wspierać wyłączenie dysków startowych z backupu maszyn wirtualnych Hyper-V z kopii zapasowych maszyn wirtualnych Hyper-V ✓ Proponowane rozwiązanie musi wspierać wyłączenie dysków danych z backupu maszyn wirtualnych Hyper-V kopii zapasowej maszyny wirtualnej ✓ Proponowane rozwiązanie musi wspierać przywracanie pojedynczego pliku z kopii zapasowej maszyny wirtualnej Hyper-V bez konieczności przenoszenia dysku wirtualnego w lokalizacji tymczasowej, jeżeli obraz kopii zapasowej jest przechowywany na taśmach ✓ Proponowane rozwiązanie musi zapewniać integrację z System Center Virtual Machine Manager (SCVMM) w celu umożliwienia odzyskiwania maszyn wirtualnych
45.	Rozwiązanie musi wspierać Nutanix: ✓ Proponowane rozwiązanie musi wspierać Nutanix Acropolis Hypervisor 5.10 i 5.11 ✓ Proponowane rozwiązanie musi wspierać co najmniej crash consistent backup maszyn wirtualnych maszyn wirtualnych Nutanix Acropolis
46.	Rozwiązanie musi wspierać RHV: ✓ Proponowane rozwiązanie musi wspierać Red Hat Virtualization 4.2.7 - 4.4.x ✓ Proponowane rozwiązanie musi wspierać spójne z aplikacjami kopie zapasowe (application consistent backups)
47.	Rozwiązanie musi wspierać Azure Stack: ✓ Proponowane rozwiązanie musi umożliwiać ochronę maszyn wirtualnych Azure Stack maszyn wirtualnych Azure Stack ✓ Proponowane rozwiązanie musi wspierać co najmniej crash consistent backup maszyn wirtualnych maszyn wirtualnych Azure Stack
48.	Rozwiązanie musi wspierać OpenStack: ✓ Proponowane rozwiązanie musi wspierać minimum następujące wersje: OpenStack • Mitaka • Newton • Ocata • Pike • Queens • Train • Rocky • Stein ✓ Proponowane rozwiązanie musi wspierać hypervisor KVM z OpenStack ✓ Proponowane rozwiązanie musi wspierać następujące dystrybucje OpenStack: • Red Hat OpenStack Platform • Huawei FusionSphere

49.	Rozwiązanie musi wspierać Docker: ✓ Proponowane rozwiązanie musi umożliwiać ochronę kontenerów Docker ✓ Proponowane rozwiązanie musi umożliwiać ochronę skonteneryzowanych aplikacji, danych aplikacji skonteneryzowanych przechowywanych na persystentnych wolumenach ✓ Proponowane rozwiązanie musi umożliwiać ochronę skonteneryzowanych danych aplikacji, danych skonteneryzowanych aplikacji z wykorzystaniem obszaru stagingowego z wykorzystaniem podejścia dump and sweep ✓ Proponowane rozwiązanie musi umożliwiać ochronę skonteneryzowanych aplikacji poprzez współlokalizację na kontenerze aplikacyjnym
50.	Rozwiązanie musi wspierać Kubernetes: ✓ Proponowane rozwiązanie musi umożliwiać ochronę i odtwarzanie danych w środowisku Kubernetes w oparciu o zarządzanie kopiami migawkowymi ✓ Proponowane rozwiązanie musi umożliwiać ochronę i odtwarzanie danych w środowisku Kubernetes z wykorzystaniem mechanizmu kopii i odtwarzania danych z kopii migawkowej ✓ Proponowane rozwiązanie musi umożliwiać tworzenie kopii zapasowych w jednej dystrybucji Kubernetes i odzyskiwanie ich w innej ✓ Proponowane rozwiązanie musi umożliwiać ochronę skonteneryzowanych aplikacji danych aplikacji skonteneryzowanych przechowywanych na persystentnych wolumenach ✓ Proponowane rozwiązanie musi umożliwiać ochronę danych aplikacji skonteneryzowanych przechowywanych na persystentnych wolumenach ✓ Proponowane rozwiązanie musi wspierać API K8s, custom operator oraz zarządzanie kopiami migawkowymi sterowanymi przez Container Storage Interface (CSI) ✓ Proponowane rozwiązanie musi umożliwić zabezpieczenie każdej bazy danych w sposób spójny aplikacyjnie ✓ Proponowane rozwiązanie musi posiadać możliwość natychmiastowego przywracania namespace Kubernetes z kopii migawkowych oraz możliwość ustawienia różnych okresów przetrzymywania dla kopii migawkowych i zapasowych ✓ Proponowane rozwiązanie musi posiadać możliwość tworzenia i zarządzanie inteligentnymi grupami zasobów Kubernetes za pomocą etykiet (label), aby zapewnić zabezpieczenie klastra Kubernetes i zasobów wraz z możliwością włączania/wyłączania zasobów z zadania kopii zapasowej
51.	Rozwiązanie musi wspierać Apache Hadoop: ✓ Proponowane rozwiązanie musi wspierać Apache Hadoop 2.5.2 - 3.1 działający na systemach Red Hat Enterprise Linux 6 i 7 oraz SUSE Linux Enterprise Server 11 i 12 ✓ Proponowane rozwiązanie nie może wymagać instalacji agentów na klastrze Hadoop (musi być bezagentowe) ✓ Proponowane rozwiązanie musi przesyłać dane bezpośrednio z wielu węzłów równolegle
52.	Rozwiązanie musi wspierać Apache HBase:

	✓ Proponowane rozwiązanie musi wspierać Apache HBase 1.2 - 2.0 działający na systemach Red Hat Enterprise Linux 6 i 7 oraz SUSE Linux Enterprise Server 11 i 12 ✓ Proponowane rozwiązanie nie może wymagać instalacji agentów na klastrze HBase na klastrze HBase (musi być bezagentowe) ✓ Proponowane rozwiązanie musi przesyłać dane bezpośrednio z wielu Region serwerów ✓ równolegle
53.	Rozwiązanie musi wspierać Apache Cassandra: ✓ Proponowane rozwiązanie musi wspierać Apache Cassandra działający na systemach Red Hat Enterprise Linux 7 i 8 ✓ Proponowane rozwiązanie nie może wymagać instalacji agentów na klastrze Cassandra (musi być bezagentowe) ✓ Proponowane rozwiązanie musi wspierać backup na gorąco i wspierać odtwarzanie pełne oraz na poziomie tabeli lub keyspace
54.	Rozwiązanie musi wspierać IBM DB2: ✓ Proponowane rozwiązanie musi wspierać IBM DB2 Universal Database 10.5 i nowsze działające na systemach IBM AIX, HP-UX, Oracle Solaris, Red Hat Enterprise Linux, SUSE Linux Enterprise Server oraz Windows ✓ Proponowane rozwiązanie musi wspierać operacje równoległego backupu i przywracania baz danych DB2 ✓ Proponowane rozwiązanie musi wspierać operacje multipleksowanego backupu i przywracania baz danych DB2 ✓ Proponowane rozwiązanie musi wspierać tworzenie kopii zapasowych typu snapshot oraz natychmiastowe przywracanie baz danych DB2 ✓ Proponowane rozwiązanie musi wspierać wykonywanie kopii zapasowych baz danych DB2 spoza serwera (off-host)
55.	Rozwiązanie musi wspierać IBM Informix: ✓ Proponowane rozwiązanie musi wspierać IBM Informix XPS i IDS ✓ Proponowane rozwiązanie musi obsługiwać równoległe operacje backupu i przywracania baz danych Informix ✓ Proponowane rozwiązanie musi obsługiwać multipleksowe backupy i restore baz danych Informix ✓ Proponowane rozwiązanie musi obsługiwać kopie zapasowe poziomu 0, 1 i 2 ✓ Proponowane rozwiązanie musi wspierać tworzenie kopii zapasowych logów logicznych
56.	Rozwiązanie musi wspierać IBM Lotus Domino: ✓ Proponowane rozwiązanie musi obsługiwać zarówno kopie zapasowe inicjowane przez politykę, jak i przez użytkownika ✓ Proponowane rozwiązanie musi wspierać IBM Lotus Domino 8 - 10 działające na systemach IBM AIX, Red Hat Enterprise Linux, SUSE Linux Enterprise Server oraz Windows ✓ Proponowane rozwiązanie musi zapewniać wykonywanie kopii zapasowych online baz danych Lotus Notes baz danych, skrzynek pocztowych oraz dzienników transakcji ✓ Proponowane rozwiązanie musi umożliwiać ochronę baz danych z partycjonowanych serwerów Domino

	✓ Proponowane rozwiązanie musi umożliwiać wznawianie nieudanego zadania backupu Domino od ostatniego punktu kontrolnego
57.	Rozwiązanie musi wspierać MariaDB: ✓ Proponowane rozwiązanie musi zapewniać ochronę baz danych MariaDB 5.5 i nowszych działających na systemach Red Hat Enterprise Linux, SUSE Linux Enterprise Server oraz Windows ✓ Proponowane rozwiązanie musi wspierać przywracanie kopii zapasowych MariaDB do klientów oryginalnych i alternatywnych
58.	Rozwiązanie musi wspierać Microsoft Exchange: ✓ Proponowane rozwiązanie musi wspierać Microsoft Exchange 2010 i późniejsze ✓ Proponowane rozwiązanie musi obsługiwać wszystkie metody backupu serwera Exchange: full, cumulative incremental oraz differential incremental ✓ Proponowane rozwiązanie musi wykonywać kopie zapasowe online Exchange bez konieczności wyłączania serwera Exchange ✓ Proponowane rozwiązanie musi obsługiwać zarówno serwery autonomiczne jak i Database Availability Groups ✓ Proponowane rozwiązanie musi umożliwiać wykonywanie kopii zapasowych Exchange spoza serwera (off-host), Instant Recovery oraz wykonywanie kopii zapasowych z wykorzystaniem sprzętowych kopii migawkowych. ✓ Zaproponowane rozwiązanie musi umożliwiać wykonywanie restartów do innej bazy danych Exchange lub na innym serwerze Exchange ✓ Proponowane rozwiązanie musi pozwalać na wykonywanie przekierowanych restartów do alternatywnych skrzynek Exchange, folderów skrzynek, wiadomości skrzynek, folderów publicznych folderów publicznych ✓ Proponowane rozwiązanie musi umożliwiać przywracanie poszczególnych elementów skrzynek i folderów publicznych bezpośrednio z dowolnej pełnej kopii zapasowej bazy Exchange
59.	Rozwiązanie musi wspierać Microsoft SharePoint: ✓ Proponowane rozwiązanie musi wspierać Microsoft SharePoint 2010 i nowsze ✓ Proponowane rozwiązanie musi wspierać ochronę SharePoint Configuration database, SSO database, Global settings, Index files, Service applications, Web applications or Content databases, Site collections, Subsites, Poszczególnych list lub bibliotek oraz Poszczególnych dokumentów lub elementów list. ✓ Proponowane rozwiązanie musi wykonywać kopie zapasowe SharePoint online bez konieczności wyłączania serwera SharePoint w trybie offline ✓ Proponowane rozwiązanie musi umożliwiać przywracanie z przekierowaniem ✓ Proponowane rozwiązanie musi umożliwiać przywracanie pojedynczych list SharePointa, elementów i zestawów dokumentów bezpośrednio z dowolnej pełnej kopii zapasowej bazy danych aplikacji webowej. ✓ Proponowane rozwiązanie musi wspierać Claims-based authentication (CBA) dla aplikacji webowych w SharePoint

60.	Rozwiązanie musi wspierać MS SQL Server: ✓ Proponowane rozwiązanie musi wspierać Microsoft SQL Server 2008 i nowsze ✓ Proponowane rozwiązanie musi wspierać SQL Server Availability Groups ✓ Proponowane rozwiązanie musi wspierać automatyczne wykrywanie instancji SQL ✓ Proponowane rozwiązanie nie powinno wymagać skryptów wsadowych tworzonych przez użytkownika, które posiadały instrukcje tworzenia kopii zapasowych instancji baz danych SQL oraz logów transakcyjnych ✓ Proponowane rozwiązanie musi zapewniać wykonywanie pełnych, różnicowych i dzienników transakcji kopii zapasowych baz danych SQL ✓ Proponowane rozwiązanie nie może wykorzystywać metody log-shipping do ochrony logów transakcyjnych SQL ✓ Proponowane rozwiązanie musi wspierać pełne przywracanie i odzyskiwanie baz danych SQL ✓ Proponowane rozwiązanie musi wspierać przywracanie grup plików SQL ✓ Proponowane rozwiązanie musi wspierać przywracanie plików bazy danych SQL ✓ Proponowane rozwiązanie musi wspierać przywracanie logów transakcyjnych SQL do określonego punktu w czasie ✓ Proponowane rozwiązanie musi wspierać przywracanie logu transakcyjnego SQL do określonego punktu w czasie konkretnej transakcji
61.	Rozwiązanie musi wspierać MySQL: ✓ Proponowane rozwiązanie musi zapewniać ochronę baz danych MySQL 5.5.5 i nowszych baz danych działających na systemach Red Hat Enterprise Linux, SUSE Linux Enterprise Server oraz Windows ✓ Proponowane rozwiązanie musi wspierać przywracanie kopii zapasowych MySQL do klientów oryginalnych i alternatywnych
62.	Rozwiązanie musi wspierać Oracle: ✓ Proponowane rozwiązanie musi wspierać bazy danych Oracle 11g R1 i nowsze działające na platformach IBM AIX, HP-UX, Oracle Linux, Oracle Solaris, Red Hat Enterprise Linux, SUSE Linux Enteprise Server oraz Windows ✓ Proponowane rozwiązanie musi integrować się z funkcjami backupu i odtwarzania baz danych Oracle Recovery Manager (RMAN) ✓ Proponowane rozwiązanie musi obsługiwać kopie zapasowe standardowych i kontenerowych baz danych Oracle ✓ Proponowane rozwiązanie musi wspierać Oracle Real Application Clusters (RAC) ✓ Proponowane rozwiązanie musi posiadać możliwość dynamicznego generowania skryptów do backupu znanych instancji Oracle ✓ Proponowane rozwiązanie musi umożliwiać wykonanie skryptu stworzonego wcześniej przez administratora do wywołania RMAN w celu wykonania kopii zapasowej bazy danych ✓ Proponowane rozwiązanie musi automatycznie generować skrypty RMAN do backupu całej bazy danych Oracle, poszczególnych przestrzeni tabel, plików danych oraz Fast Recovery Area (FRA)

	✓ Proponowane rozwiązanie musi umożliwiać konfigurację różnej ilości strumieni podczas wykonywania kopii zapasowych przestrzeni tabel lub plików danych Oracle oraz archiwalnych logów redo. ✓ Proponowane rozwiązanie musi umożliwiać dostosowanie formatów nazw plików backupu używanych przez generowane skrypty Oracle RMAN ✓ Proponowane rozwiązanie musi wspierać możliwości równoległego backupu i przywracania RMAN ✓ Proponowane rozwiązanie musi umożliwiać odtworzenie bazy danych Oracle za pomocą RMAN: • Pełne kopie zapasowe, przyrostowe kopie zapasowe poziomu 0 lub kopie plików danych • Kopia zapasowa całej bazy danych (jeśli jest wymagana) • Dowolną część bazy danych (pliki danych, przestrzenie tabel) ✓ Proponowane rozwiązanie musi dostarczać metodę klonowania baz danych Oracle ułatwiającą: • Przekierowanie plików danych • Przekierowanie plików kontrolnych • Przekierowanie logów redo • Zapewnienie walidacji operacji ✓ Proponowane rozwiązanie musi wspierać zapisywanie kopii zapasowych Oracle do i przywracanie ich z samoidentyfikującego się i niezależnego od systemu formatu np. XML
63.	Rozwiązanie musi wspierać PostgreSQL: ✓ Proponowane rozwiązanie musi zapewniać ochronę baz danych PostgreSQL 9 i nowszych działających na systemach Red Hat Enterprise Linux, SUSE Linux Enterprise Server oraz Windows ✓ Proponowane rozwiązanie musi umożliwiać przywracanie kopii zapasowych PostgreSQL do klientów oryginalnych oraz alternatywnych
64.	Rozwiązanie musi wspierać SAP: ✓ Proponowane rozwiązanie musi wspierać SAP R/3 z Oracle, SAPDB i MaxDB, oraz SAP HANA (w tym SAP HANA 2.0) ✓ Proponowane rozwiązanie musi uruchamiać wszystkie kopie zapasowe SAP oraz przywracać je jednocześnie i w sposób transparentny bez konieczności podejmowania jakichkolwiek działań przez administratora rozwiązania ✓ Proponowane rozwiązanie musi wspierać równoległe tworzenie kopii zapasowych i przywracanie możliwości SAP Tools ✓ Proponowane rozwiązanie musi integrować się z interfejsem Backint dla SAP i SAP HANA ✓ Proponowane rozwiązanie musi umożliwiać ręczne inicjowanie operacji przez administratora SAP HANA za pomocą SAP HANA Studio
65.	Rozwiązanie musi wspierać SQLite: ✓ Proponowane rozwiązanie musi zapewniać ochronę baz danych SQLite 3.10 i nowszych działających na systemach Red Hat Enterprise Linux, SUSE Linux Enterprise Server oraz Windows ✓ Proponowane rozwiązanie musi wspierać przywracanie kopii zapasowych SQLite do klientów oryginalnych i alternatywnych

66.	Rozwiązanie musi wspierać NDMP: ✓ Proponowane rozwiązanie musi wspierać wykorzystanie protokołu NDMP (Network Data Management Protocol) do inicjowania i sterowania kopiami zapasowymi i przywracaniem systemów NAS (Network Attached Storage) ✓ Proponowane rozwiązanie musi obsługiwać NDMP v2, v3 i v4 ✓ Proponowane rozwiązanie musi wykorzystywać techniki wykrywania zmian w filerze w celu identyfikacji modyfikacji, które nastąpiły od momentu wykonania ostatniego backupu ✓ Proponowane rozwiązanie musi obsługiwać lokalne i trójstronne kopie zapasowe NDMP ✓ Proponowane rozwiązanie musi obsługiwać funkcję NDMP DirectCopy ✓ Proponowane rozwiązanie musi umożliwiać przywracanie pojedynczych plików z kopii zapasowych NDMP ✓ Proponowane rozwiązanie musi obsługiwać funkcję NDMP Direct Access Recovery (DAR)
67.	Rozwiązanie musi wspierać Snapshots: ✓ Proponowane rozwiązanie musi zapewniać możliwość wykonywania migawek dla następujących macierzy dyskowych: • Pure Storage FlashArray • macierze pamięci masowej HPE 3PAR • macierze pamięci masowej NetApp • Hitachi storage array • macierze klasy enterprise InfiniBox ✓ Proponowane rozwiązanie powinno zapewniać możliwość wykonywania migawek dla następujących obciążeń w chmurze: • instancje Amazon AWS EC2 • Maszyny wirtualne Azure • Maszyny wirtualne Google ✓ Możliwość wykonywania migawek musi być dostępna dla systemów operacyjnych Windows i Linux.
68.	Rozwiązanie musi mieć możliwość raportowania: ✓ Proponowane rozwiązanie musi zapewniać podstawowe i zaawansowane raportowanie, w tym m.in. ale nie tylko; raportowanie kosztów zwrotnych, oszczędności deduplikacji, statystyki backupu, raportów o błędach, raportów na poziomie biznesowym do celów prognozowania, raportowanie SLA w zakresie backupu i odzyskiwania danych. ✓ System raportowania rozwiązania powinien umożliwiać automatyczne wysyłanie wiadomości e-mail automatycznie codziennie jako załączniki w formacie .pdf, .csv i html ✓ Proponowane rozwiązanie musi posiadać możliwość centralnego zarządzania, monitorowanie i raportowanie w odniesieniu do środowisk oprogramowania i urządzeń, w tym wielu środowisk backupowych ✓ Proponowane rozwiązanie musi umożliwiać wysyłanie powiadomień o zadaniach za pomocą poczty elektronicznej lub SNMP
69.	Odporność na Ransomware:

	✓ Proponowane rozwiązanie musi posiadać wbudowany mechanizm wykrywania i powiadamiania o podejrzanych zmianach podczas tworzenia kopii zapasowych ✓ Proponowane rozwiązanie musi posiadać własny skaner złośliwego oprogramowania oraz mieć możliwość integracji z zewnętrznymi skanerami złośliwego oprogramowania w celu skanowania składowanych obrazów kopii zapasowych ✓ Proponowane rozwiązanie musi posiadać możliwość automatycznego wstrzymywania zadań kopii zapasowych dla chronionego zasobu po wykryciu infekcji w jego kopii zapasowej, powinno obejmować tworzenie nowych kopii zapasowych, ich powielanie i wygaszanie ✓ Proponowane rozwiązanie musi posiadać możliwość identyfikowania ostatniej znanej dobrej kopii zapasowej przed przywróceniem maszyny wirtualnej ✓ Proponowane rozwiązanie musi posiadać możliwość integracji integracji z platformami SOAR/XDR w celu wstrzymywania lub wznowienia zadań związanych z ochroną danych na podstawie zdarzeń związanych z bezpieczeństwem lub pracami serwisowymi. Powiadamienia o anomaliach i skanowaniu złośliwego oprogramowania przechowywane w dziennikach oprogramowania muszą być łatwo pobierane przez systemy wczesnego ostrzegania, takie jak platformy SIEM
70.	Proponowane rozwiązanie musi umożliwiać tworzenie logicznie odizolowanych środowisk dla różnych organizacji/działów (Multi-Tenancy).
71.	Proponowane rozwiązanie musi wspierać kontrolę dostępu opartą na rolach (RBAC).
72.	Proponowane rozwiązanie musi oferować samoobsługowy backup i przywracanie danych dla wielu użytkowników, w sposób bezpieczny i podzielony na partycje.
73.	Rozwiązanie musi mieć możliwość Disaster Recovery Readiness: ✓ Proponowane rozwiązanie powinno zapewniać pojedynczy pulpit nawigacyjny do śledzenia stanu gotowości do Disaster Recovery wszystkich wybranych aplikacji. ✓ Proponowane rozwiązanie musi zapewniać pełną automatyzację wszystkich operacji związanych z niezawodnością przy udziale maszyn wirtualnych, aplikacji i wielowarstwowych usług biznesowych. ✓ Proponowane rozwiązanie powinno być w stanie zaoferować prawdziwe Disaster Recovery, jak również możliwości migracji, aby być w stanie zrealizować różne aspekty planu ciągłości biznesowej, takie jak odzyskiwanie do istniejącej i/lub zdalnej lokalizacji, migracja/odzysk do wybranej chmury publicznej. ✓ Proponowane rozwiązanie powinno umożliwiać definiowanie aplikacji wielowarstwowych, tak aby wszystkie warstwy aplikacji były migrowane do miejsca Disaster Recovery lub testowane jako jedna całość ✓ Proponowane rozwiązanie powinno być w stanie zapewnić spójne wsparcie dla platform fizycznych i wirtualnych, w tym cross-hypervisor (konwersja maszyn wirtualnych) oraz oferować opcję odzyskiwania do technologii chmurowych. ✓ Proponowane rozwiązanie powinno być w stanie zapewnić wielostanowiskową widoczność stanu zdrowia komponentów aplikacji w

	czasie rzeczywistym. stanu zdrowia komponentów aplikacji w czasie rzeczywistym ✓ Proponowane rozwiązanie powinno wspierać wiele celów poziomu usług (Service Level Objectives) w tym RPO backupu/odtwarzania ✓ Rozwiązanie powinno umożliwiać automatyczne wykonywanie procesów Disaster Recovery i odzyskiwania w trybie symulacji, bez żadnych trwałych zmian w środowisku Disaster Reovery, aby potwierdzić, że czy wszystkie wymagania są spełnione dla pomyślnego wykonania procedury Disaster Recovery. Powinno ono wspierać testy nienaruszające produkcyjną infrastrukturę ✓ Rozwiązanie DR powinno posiadać mechanizm zarządzania uprawnieniami oparte o role i powinno wykorzystywać istniejące Active Directory/LDAP do zarządzania tożsamością. ✓ Proponowane rozwiązanie musi posiadać własny mechanizm do replikacji danych, a także umożliwiać wykorzystanie mechanizmów innych producentów w celu zwiększenia elastyczności. ✓ Proponowane rozwiązanie replikacji musi obsługiwać zarówno platformy fizyczne jak i wirtualne z wbudowaną kompresją. ✓ Proponowane rozwiązanie powinno umożliwiać planowanie działań lub testów w przyszłych terminach, a rozwiązanie powinno automatycznie, bez żadnych zależności, inicjować procesy w zaplanowanych terminach. Alerty również powinny być generowane i powiadamiać administratora z wyprzedzeniem. ✓ Proponowane rozwiązanie powinno mieć możliwość zatrzymania/pauzy/wznowienia w trakcie wykonywania skonfigurowanego wcześniej procesu. ✓ Proponowane rozwiązanie powinno udostępniać status uruchomionego procesu w trakcie jego wykonywania ✓ Proponowane rozwiązanie musi zapewniać dowód zgodności z wewnętrznymi i zewnętrznymi wymogami ciągłości biznesowej za pomocą raportów z audytów i nieprzerwanych testów odzyskiwania danych po awarii w czasie rzeczywistym. ✓ Proponowane rozwiązanie musi zapewniać pełną automatyzację wszystkich operacji związanych z odpornością, w tym rejestrów uruchomień odzyskiwania oraz orkiestracji uruchamiania i zatrzymywania odzyskiwania dla aplikacji wielowarstwowych w celu zmniejszenia ryzyka przestojów spowodowanych błędami ludzkimi.

2. Urządzeni typu Appliance do Backupu z deduplikacją.

Przez Urządzenie do backupu z deduplikacją danych Zamawiający rozumie rozwiązanie charakteryzujące się jednolitą budową typu „appliance" pochodzące od jednego producenta i realizujące wszystkie wymagane funkcjonalności.

Nie dopuszcza się rozwiązania zbudowanego z niezależnych komponentów sprzętowo-programowych

Dostarczone urządzenie musi być przeznaczone do deduplikacji i przechowywania kopii zapasowych Zamawiającego.

Lp.	MINIMALNE WYMAGANIA ZAMAWIAJĄCEGO
1.	Urządzenie musi być przystosowane do montażu w szafie rack 19”
2.	Dostarczone urządzenie musi posiadać co najmniej 12 dysków SAS o rozmiarze minimum 1TB (dyski własne urządzenia)
3.	Oferowane urządzenie musi posiadać przestrzeń na dane po deduplikacji o pojemności minimum 82TB (powierzchnia czynna) z tym, że musi odbywać się to w obrębie jednego fizycznego urządzenia z półkami dyskowymi
4.	Oferowane urządzenie musi umożliwiać rozbudowę przestrzeni na dane po deduplikacji do pojemności minimum 470TB (powierzchnia czynna) z tym, że musi odbywać się to w obrębie jednego fizycznego urządzenia z półkami dyskowymi. Półki dyskowe muszą być obsadzone minimum 12 dyskami SAS, każdy o rozmiarze maksymalnie 8TB, wraz z kompletem okablowania umożliwiającego podłączenie półek zgodnie z rekomendacjami producenta
5.	Oferowane urządzenie musi posiadać minimum ✓ Min. 4 porty Ethernet 1 GbE (wymagane w urządzeniu) ✓ Min. 2 porty Ethernet 10/25 GbE z wkładkami SFP28 (wymagane w urządzeniu)
6.	Oferowane urządzenie musi mieć możliwość (przyszła rozbudowa) dostosowania konfiguracji portów do zmian w infrastrukturze LAN i SAN. Zamawiający musi mieć możliwość zmiany ilości portów urządzenia, tak by po rozbudowie posiadać kombinację: ✓ do 4 portów Ethernet 1 Gb (wymagane w urządzeniu) ✓ do 6 portów Ethernet 10/25 GbE z wkładkami SFP+ SR (wymagane w urządzeniu) ✓ do 8 portów FC 16 Gb w celu rozszerzenia funkcjonalności urządzenia o odbieranie danych od klientów systemu backupowego transmitowanych również przez SAN (wymagane w urządzeniu)
7.	Dyski z systemem operacyjnym urządzenia muszą być zabezpieczone technologią nie gorszą niż RAID 1 (lustrzana kopia wolumenu)
8.	Przechowywane kopie zapasowe oraz katalog systemu kopii zapasowych muszą być zabezpieczone technologią nie gorszą niż RAID 6 (Odporność na awarię w tym samym czasie dwóch dysków)
9.	Węzeł obliczeniowy urządzenia musi posiadać minimum 1 dysk hot-spare
10.	Każda półka dyskowa urządzenia musi posiadać minimum 1 dysk hot-spare
11.	Węzły obliczeniowe urządzenia jak i półki dyskowe muszą posiadać nadmiarowe zasilacze i wentylatory
12.	Węzły obliczeniowe urządzenia jak i półki dyskowe muszą umożliwiać wymianę dysków, zasilaczy i wentylatorów w trakcie pracy urządzenia (hot-swap)
13.	W celu optymalizacji działania i poprawy stanu zabezpieczeń urządzenia, system operacyjny urządzenia oraz zainstalowane na nim oprogramowanie musi być utwardzone (hardened) i zoptymalizowane przez jego producenta
14.	Oprogramowanie pokładowe musi umożliwiać śledzenie i zapisywanie w dzienniku zdarzeń wszystkich procesów uruchomionych na urządzeniu
15.	Konfiguracja urządzenia musi być możliwa poprzez przeglądarkę internetową i poprzez konsolę znakową

16.	Urządzenie musi obsługiwać deduplikację zarówno źródłową, jak i docelową, bez korzystania z serwerów pośredniczących, aby Zamawiający mógł wybrać miejsce deduplikacji w zależności od swoich potrzeb
17.	Urządzenie musi umożliwiać wysyłanie zdeduplikowanych i skompresowanych danych do klienta systemu kopii zapasowych bez konieczności rehydracji (proces odwrotny do deduplikacji) i dekompresji przez urządzenie, podnosząc szybkość przywracania danych, zmniejszając ilość przesyłanych danych przez medium transmisyjne i znacznie odciążając zasoby obliczeniowe urządzenia
18.	W celu uzyskania wysokiej wydajności i odciążenia sieci LAN - urządzenie musi obsługiwać backup i odtworzenia w oparciu o sieć SAN Fiber Channel, w tym bezpośrednie granularne odtworzenie ze zdeduplikowanej pamięci masowej. Urządzenia muszą obsługiwać implementację OST over FC
19.	Urządzenie musi posiadać zaimplementowane oprócz deduplikacji danych także mechanizmy optymalizujące transfer danych poprzez sieć WAN (tzw: „WAN Optimization")
20.	Urządzenie musi obsługiwać deduplikację na źródle (kliencie), na media serwerze środowiska kopii zapasowych (inline) oraz w urządzeniu (inline)
21.	Urządzenie musi oferować wiele poziomów optymalizacji procesu deduplikacji, w tym zmienną długość bloku podczas deduplikacji, automatyczną optymalizację wykorzystania procesora i pamięci, automatyczną optymalizację procesu deduplikacji w zależności od typu backupowanych danych
22.	Urządzenie musi wykonywać ciągłą kompleksową weryfikację zdeduplikowanych i przechowywanych kopii zapasowych
23.	Urządzenie musi posiadać mechanizm ciągłej weryfikacji cyklicznej kontroli nadmiarowej (CRC) danych kopii zapasowych przechowywanych w puli deduplikacji
24.	Urządzenie musi wspierać deduplikację, szyfrowanie i kompresję na źródle oraz w locie podczas zapisu na nośnik dyskowy
25.	Urządzenie musi wspierać kompresję i szyfrowanie zdeduplikowanych danych na źródle i zapisanie ich na nośnik dyskowy w niezmienionej postaci
26.	Urządzenie musi umożliwiać w przyszłości rozbudowę o funkcjonalność WORM zintegrowanej z oferowanym oprogramowaniem backupu
27.	Funkcjonalność WORM musi gwarantować ochronę obrazu kopii zapasowej tak że jest tylko do odczytu i po utworzeniu kopii zapasowej nie może być modyfikowany, uszkodzony ani zaszyfrowany oraz obraz kopii zapasowej jest chroniony przed usunięciem przed upływem terminu retencji
28.	Urządzenie z funkcjonalnością WORM musi umożliwiać obsługę przynajmniej dwóch trybów blokady okresu retencji: ✓ Nikt nie może nadpisać lub usunąć danych, które są chronione w trybie zgodności w zdefiniowanym okresie retencji. Po ustawieniu okresu przechowywania danych nie można go skrócić, można go jedynie wydłużyć. ✓ Dedykowany użytkownik może wyłączyć blokadę retencji, a następnie inny użytkownik z odpowiednimi uprawnieniami może usunąć obraz kopii zapasowej. Wszystkie zdarzenia muszą być rejestrowane w dzienniku urządzenia.

29.	Urządzenie musi posiadać wbudowany mechanizm Air Gap odcinający dostęp sieciowy do chronionych danych z wyjątkiem okresu, w którym odbywa się replikacja danych kopii zapasowych.
30.	Urządzenie musi wspierać centralne zarządzanie kluczami szyfrowania (KMS) działającym w oferowanym oprogramowaniu backupu
31.	Urządzenie musi wspierać szyfrowanie danych z wykorzystaniem minimum protokołu AES
32.	Wymagane jest dostarczenie urządzenia wraz z licencją, pozwalające na jednoczesną obsługę protokołów CIFS i NFS do pełnej pojemności urządzenia wraz z dostarczanymi półkami dyskowymi
33.	Oferowany produkt musi posiadać obsługę mechanizmów globalnej deduplikacji dla wszystkich obsługiwanych protokołów, raz otrzymany i zapisany w urządzeniu fragment danych nie może nigdy więcej zostać zapisany bez względu na to, jakim protokołem zostanie ponownie dostarczony
34.	Przestrzeń składowania duplikowanych danych musi być jedna dla wszystkich protokołów dostępowych
35.	Oferowane urządzenie musi umożliwiać asynchroniczną replikację/duplikację danych do drugiego urządzenia, konfiguracja replikacji musi być możliwa w każdym z trybów: ✓ jeden do jednego ✓ wiele do jednego ✓ jeden do wielu
36.	Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu
37.	Replikacja/Duplikacja danych między dwoma urządzeniami kontrolowana przez system backupu musi oferować następujące funkcjonalności: ✓ replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału dodatkowych serwerów ✓ replikacji podlegają tylko te fragmenty danych, które nie znajdują się w docelowym urządzeniu ✓ sterowanie odbywa się z poziomu oferowanego oprogramowania backupu ✓ oferowane oprogramowanie posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach
38.	Urządzenie musi automatycznie usuwać przeterminowane dane (fragmenty danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia
39.	Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracę procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu)
40.	Administracja i konfiguracja urządzeń musi być możliwa poprzez przeglądarkę internetową i poprzez konsolę znakową Urządzenie musi posiadać scentralizowaną konsolę zarządzania, która nie wymaga instalacji dodatkowego oprogramowania w infrastrukturze Zamawiającego.
41.	Scentralizowana konsola zarządzania musi posiadać następujące funkcjonalności: ✓ Monitorować wszystkie zainstalowane urządzenia w środowisku w jednej konsoli ✓ Udostępniać informacje o zainstalowanym sprzęcie i oprogramowaniu

	✓ Udostępniać informacje o bieżącej i historycznej (do 30 dni) utylizacji i obciążenia urządzeń ✓ Porównywać wydajność monitorowanych urządzeń ✓ Centralnie instalować nowe wersje oprogramowania urządzenia
42.	W celu optymalnego planowania pojemności środowiska kopii zapasowych, scentralizowana konsola musi dostarczać następujące informacje o monitorowanych urządzeniach: ✓ Zajętość wewnętrznej pojemności (%) ✓ Ilość obsługiwanych zadań systemu kopii zapasowych ✓ Stopień uzyskanego poziomu deduplikacji (%)
43.	W celu monitorowania i planowania wydajności środowiska kopii zapasowych, scentralizowana konsola musi dostarczać informacje o obciążeniu następujących podzespołów monitorowanych urządzeń: ✓ Procesory (%) ✓ Pamięć RAM (%) ✓ Odczyt z dysków urządzenia (MB/s) ✓ Zapis na dyski urządzenia (MB/s) ✓ Wydajność sieci (Mb/s)
44.	Scentralizowana konsola musi umożliwić eksportowanie informacji minimum w formacie CSV, tak aby była możliwość wykorzystanie informacji w systemach zewnętrznych
45.	Stan poszczególnych komponentów urządzeń musi być objęty monitorowaniem i raportowaniem w ramach narzędzia raportującego centralnego systemu kopii zapasowych stosowanego w środowisku Zamawiającego – OPS Center Analytics. Monitorowane muszą być: ✓ Temperatura panująca w urządzeniu ✓ Zasilacze ✓ Wentylatory ✓ Kontrolery RAID dysków systemowych i przechowywanych danych ✓ Karty Fiber Channel urządzenia ✓ Procesory
46.	Urządzenia muszą umożliwiać śledzenie i zapisywanie w dzienniku zdarzeń wszystkich procesów uruchomionych na urządzeniu.
47.	Architektura sprzętowa urządzeń musi być zoptymalizowana na potrzeby rozwiązań ochrony danych.
48.	System operacyjny urządzeń musi być zoptymalizowany pod kontem zadań ochrony danych i przechowywania danych.
49.	System operacyjny urządzeń musi być zoptymalizowany pod kontem bezpieczeństwa i efektywności działania. W szczególności z systemu powinny zostać usunięte wszelkie pakiety zbędne w procesach ochrony danych. W ramach dostarczonej dokumentacji rozwiązania oczekuje się wyspecyfikowania usuniętych pakietów w odniesieniu do standardowej dystrybucji oprogramowania.
50.	Producent oferowanych urządzeń musi posiadać na terenie Polski organizację serwisową świadczącą serwis zgodnie z ISO 9001 lub normą równoważną.
51.	Uszkodzone nośniki danych po wymianie pozostają własnością Zamawiającego.

52.	Serwis gwarancyjny urządzeń musi być realizowany w języku polskim przez producenta oferowanych urządzeń.

3. Wdrożenie Centralnego Systemu Kopii Zapasowych

- ✓ Modernizacja i konfiguracja nowych komponentów systemu,
- ✓ Wprowadzenie licencji,
- ✓ Integracja z AD Zamawiającego
- ✓ Inne czynności niezbędne do prawidłowego działania systemu
- ✓ Testy poprawności pracy systemu,
- ✓ Przygotowanie dokumentacji powykonawczej wraz z procedurami (disaster recovery, upgrade systemu)

4. Instruktaż z zaoferowanych komponentów systemu dla min. 2 Administratorów

- ✓ Instruktaż musi trwać minimum 2 dni każdy po 8 godzin lekcyjnych (45 minut).
- ✓ Instruktaż musi być przeprowadzone przez certyfikowanych inżynierów.
- ✓ W trakcie szkolenia dla uczestników szkolenia w ciągu dnia, musi być dostarczony minimum jeden posiłek ciepły i dwie przerwy kawowe.
- ✓ Instruktaż musi być przeprowadzony w formie, gdzie minimum 50% czasu szkolenia to będą warsztaty praktyczne.
- ✓ Warsztaty muszą być przeprowadzone na infrastrukturze Zamawiającego.
- ✓ Instruktaż musi być przeprowadzony w języku polskim.
- ✓ Dla każdego uczestnika szkolenia muszą zostać dostarczone materiały szkoleniowe w formacie przeszukiwalnym.
- ✓ Dopuszcza się szkolenie w formie online.

Załącznik nr 2 do zapytania o wycenę

FORMULARZ WYCENY

Wykonawca (pełna nazwa albo imię i nazwisko)		
Siedziba/miejsce zamieszkania i adres jeżeli jest miejscem wykonywania działalności Wykonawcy		
numer KRS (w zależności od podmiotu)		
NIP/REGON		
Imię nazwisko, stanowisko/podstawa **do reprezentacji**		
telefon		
e-mail		
Osoba do kontaktów z Zamawiającym		
Czy Wykonawca jest mikroprzedsiębiorstwem bądź małym lub średnim przedsiębiorstwem[1]?	[ ] Tak / [ ] Nie	Mikroprzedsiębiorstwo
	[ ] Tak / [ ] Nie	Małe przedsiębiorstwo
	[ ] Tak / [ ] Nie	Średnie przedsiębiorstwo

Ministerstwo Edukacji i Nauki

ul. Wspólna 1/3

00-529 Warszawa

W odpowiedzi na zapytanie o wycenę na **rozbudowę Centralnego Systemu Kopii Zapasowych wraz z appliance oraz 3-letnim wsparciem producenta** (znak: BDG-WII.072.3.2023), przedstawiam wycenę jak niżej:

[1]**Por.** ***zalecenie Komisji z dnia 6 maja 2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz.U. L 124 z 20.5.2003, s. 36). Te informacje są wymagane wyłącznie do celów statystycznych. Mikroprzedsiębiorstwo: przedsiębiorstwo, które zatrudnia mniej niż 10 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 2 milionów EUR. Małe przedsiębiorstwo: przedsiębiorstwo, które zatrudnia mniej niż 50 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 10 milionów EUR. Średnie przedsiębiorstwa: przedsiębiorstwa, które nie są mikroprzedsiębiorstwami ani małymi przedsiębiorstwami*** **i które zatrudniają mniej niż 250 osób i których roczny obrót nie przekracza 50 milionów EUR** ***lub*** **roczna suma bilansowa nie przekracza 43 milionów EUR.**

Lp.	*Przedmiot zamówienia*	*szt.*	*Cena jednostkowa (netto) PLN*	*Wartość netto PLN (kol. 3 x kol. 4)*	*Podatek od towarów i usług*	*Wartość (brutto) PLN (kol. 5 + kol. 6)*
1	*2*	*3*	*4*	*5*	*6*	*7*
1	Appliance …… ***wyceniany model***	1	……	……	…. %	……..
2	3-letnia subskrypcja na licencje Appliance …… ***nazwa wycenianej licencji***			……	…. %	……..
3	3-letnie wsparcie na Appliance …… ***nazwa wycenianej licencji***			……	…. %	……..
4	Przedłużenie wsparcia na posiadane licencje na 3 lata: NETBACKUP PLATFORM BASE COMPLETE ED WITH FLEXIBLE LICENSING XPLAT 1 FRONT END TB PLUS ONPREMISE STANDARD PERPETUAL LICENSE GOV …… ***nazwa wycenianej licencji***	7	……	……	…. %	……..
5	Przedłużenie wsparcia na posiadane licencje na 3 lata: NETBACKUP PLATFORM BASE COMPLETE ED WITH FLEXIBLE LICENSING XPLAT 1 FRONT END TB PLUS ONPREMISE STANDARD PERPETUAL LICENSE CORPORATE …… ***nazwa wycenianej licencji***	4	……	……	…. %	……..
6	Przedłużenie wsparcia na posiadane licencje na 3 lata: NETBACKUP PLATFORM BASE COMPLETE ED XPLAT 1 FRONT END TB ONPREMISE STANDARD PERPETUAL LICENSE CORPORATE …… ***nazwa wycenianej licencji***	3	……	……	…. %	……..
7	Nowe licencje …… ***nazwa wycenianej licencji***	14	……	……	…. %	……..
8	3-letnie wsparcie na nowe licencje …… ***nazwa wycenianej licencji***	14	……	……	…. %	……..
9	Wdrożenie			……	…. %	……..
10	Instruktaż			……	…. %	……..
			RAZEM	……	…. %	……..
brutto słownie złotych: ……						

data ……

……
podpis osoby/osób uprawnionej/uprawnionych do reprezentowania Wykonawcy

Informacja dla Wykonawcy: Formularz wyceny musi być podpisany przez osobę lub osoby uprawnione do reprezentowania Wykonawcy podpisem własnoręcznym - wówczas oferta składana jest w formie skanu lub podpisem w formie elektronicznej (kwalifikowany podpis elektroniczny).

Załącznik nr 4 do zapytania o wycenę

Postępowanie o udzielenie zamówienia publicznego pn. **Rozbudowa Centralnego Systemu Kopii Zapasowych wraz z appliance oraz 3-letnim wsparciem producenta** (sprawa: BDG-WII.072.3.2023), prowadzone z wyłączeniem stosowania ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych

Klauzula informacyjna dot. przetwarzania danych osobowych przez Zamawiającego

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2), dalej „RODO", informuję, że:

1) administratorem Pani/Pana danych osobowych jest Ministerstwo Edukacji i Nauki;
2) dane kontaktowe do inspektora ochrony danych w Ministerstwie Edukacji i Nauki: Ministerstwo Edukacji i Nauki, ul. Wspólna 1/3, 00-529 Warszawa, adres e-mail: inspektor@mein.gov.pl;
3) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z przeprowadzeniem postępowania o udzielenie zamówienia publicznego jak również zawarcia umowy w sprawie zamówienia oraz jej realizacji, a także udokumentowania postępowania o udzielenie zamówienia i jego archiwizacji;
4) odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym dokumentacja postępowania zostanie udostępniona /osoby lub podmioty zapewniające obsługę informatyczną Ministerstwa Edukacji i Nauki / wszystkie osoby, które zapoznają się z informacjami zamieszczonymi na stronie internetowej MEiN;
5) Pani/Pana dane osobowe będą przechowywane do czasu ustania celu jakim jest przeprowadzenie postępowania o udzielenie zamówienia, zawarcie i wykonanie umowy, a następnie, jeśli chodzi o materiały archiwalne, zgodnie z Instrukcją Kancelaryjną Ministerstwa Edukacji i Nauki oraz przepisami o archiwizacji dokumentów – przez okres co najmniej 5 lat od dnia przekazania ich do archiwum Ministerstwa Edukacji i Nauki;
6) obowiązek podania przez Panią/Pana danych osobowych jest wymogiem związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego;
7) w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
8) posiada Pani/Pan:
   - na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących,
   - na podstawie art. 16 RODO prawo do sprostowania lub uzupełnienia Pani/Pana danych osobowych,
   - na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych,
   - prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO.