Załącznik Nr 1 do SWZ

SPECYFIKACJA TECHNICZNA ZAMÓWIENIA

1. Stacje robocze – 8 sztuk

Specyfikacja

Specyfikacja sprzętu:	Parametry (co najmniej):
Obudowa	Obudowa fabrycznie przystosowana do pracy w pozycji pionowej typu Small Form Factor posiadająca min.: półkę 1 szt. dla napędu optycznego typu SLIM, 1 wewnętrzną półkę umożliwiającą montaż jednego dysku twardego 3,5” lub dwóch szt. dysków 2,5”. Zaprojektowana i wykonana przez producenta komputera opatrzona trwałym logo producenta, metalowa. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady typu Kensington) oraz kłódki (oczko na kłódkę) a także być wyposażona w śrubę serwisową. Zasilacz o mocy min. 180 W i sprawności min 92% przy 50% obciążeniu zasilacza (80 Plus Gold).
Procesor	Min. 6-rdzeniowy, osiągający w zaoferowanej konfiguracji w teście PassMark CPU Mark wynik min. 31158 punktów. Zestaw instrukcji: 64-b
Obsługa technologii vPro	Tak
Pamięć zainstalowana	8 GB DIMM DDR4, 3200 MHz
Liczba banków pamięci RAM	2
Możliwość obsługi pamięci RAM	32 GB
Pojemność dysku	512 GB
Parametry dysku	NVMe PCI Express M.2 Możliwość obsługi dysków SATA
Karta graficzna	zintegrowana
Trusted Platform Module (TPM)	TAK
Złącza – panel tylni	USB 2.0 - 2 szt. USB 3.2 Gen. 1 - 2 szt. Wyjście słuchawkowe/głośnikowe - 1 szt. RJ-45 (LAN) - 1 szt. HDMI - 1 szt. Display Port - 1 szt.

Złącza – panel przedni	USB 2.0 - 2 szt. USB 3.2 Gen. 1 - 2 szt. Wyjście słuchawkowe/wejście mikrofonowe
Łączność	Wi-Fi 5 (802.11 a/b/g/n/ac) LAN 10/100/1000 Mbps Bluetooth
BIOS	BIOS zgodny ze specyfikacją UEFI Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji o: - modelu komputera, PN - numerze seryjnym, - Numer inwentarzowy, - MAC Adres karty sieciowej, - wersja i data BIOS - zainstalowanym procesorze, jego taktowaniu i ilości rdzeni - ilości pamięci RAM, - stanie pracy wentylatora - informacja o licencji na system operacyjny Możliwość z poziomu Bios: - wyłączenia/włączenia selektywnego (pojedynczo) portów USB zarówno z przodu jak i z tyłu obudowy oraz z boku obudowy. - wyłączenia karty sieciowej (WIFI i LAN), karty audio, mikrofonu, kamery, czytnika kart multimedialnych - możliwość wyłączenia wirtualizacji w BIOS - możliwość zaprogramowania automatycznego włączenia komputera o określonej porze - możliwość ustawienia następujących haseł: hasła administratora, hasła Power-On, hasła na dysk twardy - dostęp do systemu logowania zdarzeń w BIOS. System musi zapewniać logowanie co najmniej takich zdarzeń jak: update BIOS, zmiany w konfiguracji, wyczyszczenie logów - obsługa Bios za pomocą klawiatury i myszy

Dodatkowe wymagania	Komputer musi posiadać wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający na wykonanie diagnostyki następujących podzespołów: · wykonanie testu pamięci RAM · test dysku twardego · test monitora · test płyty głównej Wizualna lub dźwiękowa sygnalizacja w przypadku błędów któregokolwiek z powyższych podzespołów komputera. Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie: · PC: Producent, model · Procesor: Nazwa, taktowanie · Pamięć RAM: Ilość zainstalowanej pamięci RAM, producent oraz numer seryjny poszczególnych kości pamięci · Dysk twardy: model, numer seryjny, wersja firmware, pojemność, temperatura pracy System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera. Urządzenia muszą posiadać: - Certyfikat ISO 9001 dla producenta sprzętu lub równoważny - Certyfikat ISO 14001 dla producenta sprzętu lub równoważny - Certyfikat ISO 50001 dla producenta sprzętu lub równoważny - Certyfikacja EPEAT lub równoważny - Deklaracja zgodności CE lub równoważny
Napęd DVD	Tak
Akcesoria dodatkowe	Mysz przewodowa producenta komputera Klawiatura przewodowa producenta komputera
System operacyjny	Zgodnie ze specyfikacją dla stacji roboczych

Specyfikacja – system operacyjny stacje robocze:

1. System operacyjny spełniający wymagania:
   - Możliwość dokonywania aktualizacji i poprawek systemu przez Internet; możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu;
   - Aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) z mechanizmem sprawdzającym, które z poprawek są potrzebne;
   - Internetowa aktualizacja zapewniona w języku polskim;
   - Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IPSec v4 i IPSec v6;
   - Zlokalizowane w języku polskim, min. elementy: menu, przeglądarka internetowa, klient poczty elektronicznej z kalendarzem spotkań, pomoc, komunikaty systemowe;
   - Wsparcie dla powszechnie używanych urządzeń (drukarek, urządzeń sieciowych, USB, Plug&Play, Wi-Fi, etc.);
   - System działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta;
   - Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim;
   - Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;
   - Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony konta użytkownika;
   - Zintegrowane z systemem:
     - moduły wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych;
     - narzędzia do zwalczania złośliwego oprogramowania; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych;
     - moduły do pracy grupowej uruchamiany ad-hoc w zależności od potrzeb;
     - moduły synchronizacji komputera z urządzeniami zewnętrznymi;
   - Dostępne w systemie zasoby wskazujące jak wykorzystać funkcje systemu w zastosowaniach biznesowych;
   - Wbudowany system pomocy w języku polskim;
   - Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
   - Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji;
   - Wdrażanie IPSec oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
   - Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509, certyfikat EAL 4 dla systemu operacyjnego zarządzanych w sposób centralny;
   - Wsparcie dla logowania przy pomocy smartcard;
   - Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji;

- Narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;
- Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0, 3.0 i 4.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach;
- Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń;
- Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem;
- Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe;
- Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, woluminy dyskowe, usługi katalogowe;
- Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej;
- Możliwość przywracania plików systemowych;
- Funkcjonalność pozwalającą na identyfikację sieci komputerowych do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.);
- Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (przy użyciu numerów identyfikacyjnych sprzętu);
- Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie **TPM** (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB;
- Systemowe narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych;
- Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.
  - Klucz licencyjny zapisany trwale w **BIOS** umożliwiający instalację systemu operacyjnego na podstawie dołączonego nośnika bezpośrednio z wbudowanego napędu lub zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego.

2. Dołączone do oferowanego komputera oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające:
   - upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,
   - sprawdzenia przed instalacją każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem.

2. Serwer wraz z systemem operacyjnym – 1 sztuka

Specyfikacja

Specyfikacja sprzętu:	Parametry (co najmniej):
Obudowa	Rack
Szyny montażowe	TAK - wysuwane z prowadnicami kabli umożliwiającymi wysunięcie serwera do celów serwisowych.
Wysokość	1U
Ilość gniazd procesora	2
Procesor	16-rdzeniowy klasy x86 - 64 bity, o taktowaniu min. 2.4 GHz osiągający w zaoferowanej konfiguracji w teście PassMark CPU Mark wynik min. 29 000 punktów.
Ilość zainstalowanych procesorów	1
RAM	128 GB w minimum czterech bankach pamięci po min 32GB
Kontroler RAID sprzętowy	TAK z min 4GB pamięci i NV cache
Poziomy RAID	0/1/5/6/10/50/60
Wsparcie PCI	PCIe Gen. 4
Dyski	4x 960 SSD o DWPD = min 1
Interfejs	SATA 6Gb/s
Karta sieciowa	Wbudowane zintegrowane min 2 porty 1Gb/s ,oraz dodatkowe 2 porty 10Gb SFP+ nie zajmujące portów PCI-e
Zasilacz [moc]	Dwa redundantne zasilacze o mocy max 600W
Typ zasilacza	Hot-Plug
Tryb redundancji	TAK
System operacyjny	wg specyfikacji
Zdalne zarządzanie , przejęcie zdalnej konsoli KVM, zdalne montowanie obrazów ISO	TAK jeśli wymagana jest dodatkowa licencja , należy ją dostarczyć na tym etapie zamówienia
Dodatkowe oprogramowanie	Licencja Vmware Essentials Kit na 1 rok
Dodatkowe wymagania:	Urządzenie musi posiadać: - Certyfikat ISO 9001 dla producenta sprzętu lub równoważny - Certyfikat ISO 14001 dla producenta sprzętu lub równoważny - Certyfikat ISO 50001 dla producenta sprzętu lub równoważny - Deklaracja zgodności CE lub równoważny

Dokumentacja, inne:

1) Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA
2) Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Polsce.
3) Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, (ogólnopolski numer o zredukowanej odpłatności 0-800/0-801, w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;
4) Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera.

Specyfikacja - Serwerowy system operacyjny.

Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym, umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze.
Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy:

1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym;
2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny;
3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych;
4) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci;
5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy;
6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy;
7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego;
8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;
9) Wbudowane wsparcie instalacji i pracy na wolumenach, które:
   a) pozwalają na zmianę rozmiaru w czasie pracy systemu,
   b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
   c) umożliwiają kompresję „w locie” dla wybranych plików i/lub folderów,
   d) umożliwiają zdefiniowanie list kontroli dostępu (ACL);
10) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość;
11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji;
12) Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET;

13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów;
14) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych;
15) Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    a) klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    b) dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe;
17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji;
18) Mechanizmy logowania w oparciu o:
    a) login i hasło,
    b) karty z certyfikatami (smartcard),
    c) wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM);
19) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych;
20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play);
21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu;
22) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa;
23) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management);
24) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach;
25) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    a) podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
    b) usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
        - podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
        - ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
        - odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
        - bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1,
    c) zdalna dystrybucja oprogramowania na stacje robocze,
    d) praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,
    e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
        - dystrybucję certyfikatów poprzez http,
        - konsolidację CA dla wielu lasów domeny,
        - automatyczne rejestrowanie certyfikatów pomiędzy różnymi lasami domen,
        - automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509,
    f) szyfrowanie plików i folderów,

g) szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
h) możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,
i) serwis udostępniania stron WWW,
j) wsparcie dla protokołu IP w wersji 6 (IPv6),
k) wsparcie dla algorytmów Suite B (RFC 4869),
l) wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
m) wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
   - dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
   - obsługi ramek typu jumbo frames dla maszyn wirtualnych,
   - obsługi 4-KB sektorów dysków,
   - nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,
   - możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API,
   - możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode);

26) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet;
27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath);
28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego;
29) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty;
30) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF;
31) Zorganizowany system szkoleń i materiały edukacyjne w języku polskim;
32) Serwerowy system operacyjny w najnowszej wersji producenta oprogramowania dostępnej na rynku.

Wdrożenie systemu serwerowego
Specyfikacja
Wdrożenie obejmie:
Instalacja serwera obejmie m.in.:
- instalacja i konfigurację podzespołów
- instalacja i konfigurację dysków oraz ich trybu pracy RAID kontrolera
- podłączenie do istniejącej sieci
- instalację oraz konfigurację oprogramowania Vmware Essenstials Kit
- instalację oraz konfigurację systemu operacyjnego

3. System składowania i archiwizacji danych oraz wykonywania kopii zapasowych wraz z oprogramowaniem - 1 sztuka (urządzenie typu NAS wraz z dyskami twardymi)

Specyfikacja urządzenia typu NAS

Specyfikacja sprzętu:	Parametry (co najmniej):
Częstotliwość procesora	Min. 1,7 GHz
Ilość rdzeni/wątków	4/8
Architektura	64 bit
Pamięć RAM	4 GB
Rodzaj pamięci	DDR4
Ilość wnęk 3,5”	8
Interfejs dysków	SATA 6 Gb/s, 3 Gb/s
Złącza	USB 3.0 – 3 szt.
Porty RJ-45 2,5 Gb/s	2
Porty RJ-45 10 Gb/s	2
Wake on LAN	TAK
Obudowa	Tower
Ilość dysków dostarczonych	4, przeznaczone do NAS
Wielkość dysku	6 TB
Prędkość obrotowa	7200 obr/min
Pamięć podręczna	256 MB
Nominalny czas pracy	1 mln godzin
Technologia zapisu	CMR
Dodatkowe wymagania	Deklaracja zgodności CE lub równoważny

Oprogramowanie specjalistyczne do kopii zapasowych

Specyfikacja:

Wymogi funkcjonalne dla systemu zarządzania danymi obejmujące: backup serwerów fizycznych, aplikacji oraz maszyn wirtualnych.

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 - nie zintegrowanych pomiędzy sobą, wymagających wykorzystywania różnych konsol dla zarządzania czy konfiguracji.
Zamawiający rozumie archiwizację danych, jako proces przenoszenia zasobów plikowych do archiwum (repozytorium dyskowe lub taśmowe) po skopiowaniu tych zasobów system musi tworzyć skróty oraz kasować zarchiwizowane dane.
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.

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 całość oferty, z tym iż licencje dla silnika bazodanowego muszą pozwalać na zainstalowanie go: na serwerze fizyczny (minimum 2xCPU po 8 core), klastrze active-passive czy serwerze wirtualnym w środowisku Vmware i Hyper-V.
4. Licencje muszą pozwalać na stworzenie dla serwera zarządzającego rozwiązania wysokodostępnego, z czasem przełączenia nie dłuższym niż 15 minut. Jeśli do stworzenia takiego 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. Rozwiązanie musi zapewnić interfejs graficzny do zarządzania i instalacji.
6. 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 binarii klienckich
7. System musi zapewniać funkcjonalność odtwarzania, po awarii, konfiguracji serwera zarządzającego tworzeniem kopii bezpieczeństwa i archiwów.
8. System musi posiadać możliwość nieodwracalnego kasowania danych – funkcjonalność ta musi być częścią oprogramowania.
9. 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.
10. System musi pozwalać na zarządzanie całością działania systemu (backup, archiwizacja, backup stacji roboczych) z jednej konsoli administracyjnej oraz także z konsoli webowej.
11. Agenci systemu muszą posiadać funkcjonalność komunikowania się poprzez jeden port TCP/IP, celem zabezpieczenia komunikacji z środowisk typu DMZ.
12. Automatyczne tunelowanie komunikacji TCP/IP pomiędzy agentami systemu – jeśli agent systemu wykryje ograniczenia w komunikacji, automatycznie zestawia połączenie tunelowe.
13. System musi umożliwiać konfigurację, którymi kartami sieciowymi ma przebiegać komunikacja i transfer danych, wybór interface musi odbywać się co najmniej poprzez nazwę domeny, subnet, zakres IP.
14. Komunikacja agentów systemu z serwerami musi odbywać się poprzez SSL – konfiguracja tego typu transferu nie może powodować konieczności instalowania dodatkowego oprogramowania.

15. System musi umożliwić przechowywanie jedynie unikalnych bloków danych tzw. deduplikacja. Funkcjonalność ta musi działać na poziomie blokowym i być wykonywana online podczas procesu tworzenia kopii danych. Deduplikacja musi być realizowana poprzez oprogramowanie systemu na dowolnym sprzęcie czy to w warstwie serwera systemu czy klienta. Pojedynczy serwer systemu musi umożliwiać przechowywanie danych po deduplikacji minimum do 500 TB (rozbudowa do tej wielkości może nastąpić tylko poprzez dodanie dodatkowej przestrzeni do składowania danych poprzez dodanie dysków, półki dyskowej a nie przez wymianę urządzenia).
16. Włączenie funkcjonalności deduplikacji na kliencie musi być możliwe dla różnych systemów operacyjnych: Windows, Linux, Unix i Macintosh.
17. Logiczna globalna deduplikacja – system musi oferować deduplikację globalną co oznacza iż niezależnie od tego, z jakich klientów dane będą deduplikowane (serwery fizyczne, hosty wirtualne, bazy i aplikację) – deduplikacja musi opierać się na jednej logicznej centralnej bazie deduplikacyjnej
18. 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 dla uzyskania funkcjonalności deduplikacji danych.
19. System musi zapewniać wspólny stopień deduplikacji (jedna baza deduplikacyjna) dla danych czy to z backupu czy archiwizacji.
20. 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.
21. 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.
22. System musi zapewniać dostęp zintegrowany z usługą katalogową, minimum to Active Directory, a więc tak zwany „single sign on” – pojedyncze logowanie: użytkownik po zalogowaniu do domeny AD, nie potrzebuje wykonywać następnego logowania aby zarządzać systemem poprzez konsolę administracyjną.
23. 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.
24. System musi pozwalać na zarządzanie z poprzez konsolę wiersza poleceń z tym, że uruchomienie jakiejkolwiek komendy/polecenia musi zostać poprzedzone koniecznością zalogowania (autentyfikacji) do systemu, funkcjonalność musi dotyczyć dowolnej platformy (minimum Windows/Linux) i nie może polegać na konieczności instalowania czy konfigurowania dodatkowych komponentów np. SSH.
25. Komunikacja pomiędzy agentem a serwerem systemu musi opierać się na certyfikatach. 26. System musi posiadać funkcjonalność blokowania danych do odczytu dla administratora, to znaczy, że administrator systemu nawet mając pełne uprawnienia nie może odtworzyć danych, jeśli nie jest ich właścicielem, funkcjonalność ta musi być dostępna nie tylko dla danych z laptopów/desktopów ale i dla serwerów (także dla danych plikowych i bazodanowych).
27. System musi pozwalać na skonfigurowanie mechanizmu podwójnej autentyfikacji administratora – do uruchomienia konsoli administracyjnej systemu potrzebne jest nie tylko logowanie, ale i dodatkowy tymczasowy kod wysyłany do administratora np. poprzez mail.
28. Szyfrowanie danych musi pozwalać na wybór algorytmu (minimum dwa algorytmy: Blowfish, AES) także dla danych deduplikowanych na kliencie systemu.
29. System musi wspierać mechanizm szyfrowania danych na napędach taśmowych LTO.
30. System musi pozwalać na ustawianie haseł dostępu do nośników tzw: media password.
31. 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.

32. System musi mieć wbudowane mechanizmy zabezpieczające przed złośliwym oprogramowaniem (Ransomware), minimum to:
    1) Zabezpieczenie ścieżek dostępu do danych składowanych (kopii backupowych) na dyskach – tylko procesy systemu mogą zapisywać i modyfikować dane;
    2) Monitorowanie nietypowych aktywności na serwerach za pomocą np. metody: Honeypot;
    3) Monitorowanie nietypowych aktywności na serwerach plikowych i desktopach, monitorowanie musi odbywać się nie rzadziej, niż co 5 minut i każdy niestandardowy wynik jest automatycznie wysyłany w postaci alertu lub notyfikacji;
    4) Air Gap (izolowanie i segmentowanie składowanych kopii backupowych) – musi polegać na wbudowanym automatycznym mechanizmie wyłączania komunikacji pomiędzy pozostałymi komponentami systemu backupowego. Tak więc komunikacja z wybranym segmentem środowiska backupowego odbywa się tylko w określonym przedziale czasowym dla potrzeb replikacji kopii backupowych, natomiast przez pozostały czas żadne procesy systemu backupowego nie mają możliwości komunikacji z tym środowiskiem;
    5) Możliwość definiowania serwerów komunikacyjnych (tzw. bram/gateway) przez które wykonywana jest komunikacja pomiędzy modułami systemu backupowego, w szczególności pomiędzy serwerem zarządzającym a serwerem medii czy serwerem z dowolnym agentem backupowym;
    6) Możliwość definiowania kierunki inicjalizowania komunikacji sieciowej pomiędzy komponentami systemu backupowego;
    7) Możliwość zablokowania zmiany retencji (czas przechowywania kopii backupowych) na krótszą dla kopii backupowych składowanych na dowolnych typach nośników w tym na dyskach i taśmach.
33. System musi posiadać rozbudowany system powiadamiania o zdarzeniach poprzez email.
34. System musi automatycznie wysyłać informacje o alertach, zdarzeniach oraz informacjach audytowych do syslog serwera.
35. System musi posiadać rozbudowany system raportowania dla administratorów, minimalny zestaw dostępnych raportów to:
    1) Raport zmian/wzrostu środowiska systemu;
    2) Raport wykorzystania licencji;
    3) Raport wykonanych zadań backupowych.
36. System musi mieć możliwość automatycznego zapisywania raportów w formacie minimum: PDF, HTML i CSV.
37. System musi pozwalać na definiowanie alertów per zadanie backupowe lub zadanie odtwarzania danych
38. System musi zapewniać funkcjonalność wznawiania zadań backupowych.
39. 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.
40. System musi zapewniać funkcjonalność multipleksowania kilku strumieni danych na nośniku taśmowym – tzw. multiplexing. Wydajny zapis wielu strumieni danych na taśmy bez pośrednictwa dysków.
41. System musi oferować funkcjonalność backupu blokowego, polegającego na tym, iż agent buduje własną bazę zmian bloków danych, przez co backup przyrostowy nie wymaga odczytu całych plików tylko zmienionych bloków wielokrotnie przyspieszając backup.
    Funkcjonalność ta musi być dostępna dla backupu danych plikowych.
42. System musi posiadać funkcję szyfrowania i kompresji danych transmitowanych przez LAN, możliwość wykorzystania szyfrowania i kompresji musi być dostępna w dowolnej kombinacji.
43. 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 (restore).

44. System musi posiadać (jako opcja) zintegrowane w systemie mechanizmy indeksowania pełnokontekstowego i wyszukiwania danych. Indeksowaniu powinny podlegać dane zbackupowane i zarchiwizowane już znajdujące się w systemie.
45. System musi realizować funkcjonalność weryfikacji wykonanych kopii.
46. System powinien umożliwiać wykorzystanie funkcjonalności Bare Metal Restore dla odtwarzania systemu po awarii, wsparcie musi być dostępne dla systemów:
    1) Windows;
    2) Linux;
    3) Unix: AIX'
    4) OpenVMS/
47. System musi umożliwiać integrację z mechanizmami kopii migawkowych czołowych producentów pamięci masowych minimum: HDS, Dell, HP, NetApp, EMC, IBM, Pure Storage, Nimble Storage, z tym że takowy backup sterowany przez system a wykonywany przez daną macierz dyskową musi być dostępny nie tylko dla zasobów plikowych ale i aplikacji.
48. System powinien umożliwiać (jako opcja) obsługę urządzeń składowania danych w chmurze, minimum: Azure, Amazon, Google Cloud, jeśli do włączenia tej funkcjonalności potrzebne są jakieś dodatkowe komponenty to muszą być zaoferowane
49. System musi umożliwiać odtwarzanie danych plikowych pomiędzy systemami operacyjnymi np. odtwarzanie danych plikowych Linux na systemie Windows.
50. System musi pozwalać na odtwarzanie tylko samych uprawnień do plików.
51. System musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL).
52. System musi wspierać wykonanie kopii na systemach klasy Windows, Linux i Unix.
53. System musi posiadać szerokie wsparcie dla środowisk Linux, minimum: RHEL, SuSe, Debian, Fedora, Gentoo, Mandriva, Oracle Linux, Ubuntu, Slackware.
54. System musi posiadać szerokie wsparcie dla środowisk Unix, minimum: AIX, FreeBSD, HP-UX, Solaris.
55. System musi umożliwiać uruchamianie skryptów przed i po backupie, z tym iż musi posiadać mechanizm definiowania konta użytkownika na którym te skrypty byłyby uruchamiane. Mechanizm ten musi być centralnie zarządzany poprzez konsolę administracyjną. Niedopuszczalna jest konieczność np. zmiany konta serwisowego dla danego agenta – konta serwisowe muszą być centralnie definiowane i zarządzane. 56. System musi wspierać backup całym maszyn wirtualnych/kontenerów dla czołowych rozwiązań wirtualizacyjnych, kontenerowych i chmurowych: Amazon, Citrix Xen, Google
    Cloud Platform, Microsoft Azure, Microsoft Hyper-V Kubernetes, Nutanix Acropolis
    Hypervisor (AHV), Oracle VM,Red Hat Virtualization, vCloud Director, VMware (streaming and IntelliSnap).Oznacza to, że system musi posiadać dedykowany komponent do backupu minimum całej maszyny wirtualnej/kontenera/aplikacji/wolumenu bez konieczności instalowania agenta wewnątrz np. maszyny z możliwością granualnego odtwarzania pojedynczych plików.
57. System musi wspierać wersje środowisk VMware 4.1, 5.0.x, 5.1.x, 5.5, 5.5.1, 5.5.2, 5.5.3, 6.0, 6.0.1, 6.5, 6.7, 7.0 poprzez integrację z vStorage API.
58. 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.
59. System musi wspierać środowisko Hyper-V dla:
    1) Microsoft Windows Server 2012 R2;
    2) Microsoft Hyper-V Server 2012 R2;
    3) Microsoft Windows Server 2016 (z Core Edition);
    4) Microsoft Hyper-V Server 2016 (z Core Edition);
    5) Microsoft Windows Server, version 1709 (z Core Edition);
    6) Microsoft Hyper-V Server, version 1709 (z Core Edition);
    7) Microsoft Windows Server 2019 (z Core Edition); 8) Microsoft Hyper-V Server 2019

(z Core Edition). 9) Microsoft Windows Server 2022 (z Core Edition); 10) Microsoft Hyper-V Server 2022 (z Core Edition).

60. System musi zapewniać automatyczne wykrywanie i dodawanie do polityki backupu nowych maszyn wirtualnych.
61. System musi umożliwiać odzyskanie i uruchomienie maszyn wirtualnych z kopii zapasowej bez oczekiwania na pełne przywrócenie maszyny wirtualnej minimum dla Vmware i Hyper-V.
62. System musi umożliwiać konwertowanie maszyn wirtualnych pomiędzy wirtualizatorami, minimum:
    1) Vmware do: Hyper-V, Azure, Amazon, Google Cloud Platform, Openstack, Oracle Cloud Infrastructure;
    2) Hyper-V do: Azure, Amazon, Vmware; 3) Amazon do: Azure, Vmware;
    4) Azure do: Amazon, Hyper-V, Vmware;
63. System musi wspierać mechanizm CBT (change block tracking) minimum dla Vmware i Hyper-V.
64. System musi umożliwiać konwersję zbackupowanego serwera Windows i Linux do maszyny wirtualnej w środowisku:
    1) Hyper-V; 2) Vmware.
65. System musi umożliwiać wykonanie kopii na gorąco bazy danych MySQL, Postgress, 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.
66. System musi umożliwiać wykonanie kopii na gorąco bazy danych MS SQL, Oracle, MySQL, Postgress, 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. 67. Odtwarzanie danych z backupu bazodanowego (MS SQL, Oracle, MySQL, Postgress, DB2, Informix) musi odbywać się poprzez konsolę administracyjną bez konieczności konfigurowania skryptów.
68. Dla silników bazodanowych MS SQL, Oracle i SAP HANA musi istnieć mechanizm backupu logów transakcyjnych z częstotliwością co 1 minuta, nawet w przypadku, gdy serwer zarządzający systemem backupowym jest niedostępny
69. Konfiguracja agentów backupowych dla: MS SQL, Oracle, mySQL musi odbywać się poprzez interface 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.
70. System musi umożliwiać wykonanie kopii na gorąco Active Directory a następnie odzyskania pojedynczych obiektów AD wraz z hasłami użytkowników.
71. System musi umożliwiać odtwarzanie backupu wykonywanego online dedykowanym agentem, do pliku celem późniejszego odtwarzania bez udziały systemu. Funkcjonalność ta musi być dostępna minimum dla MS SQL, Oracle i Exchange.
72. System musi umożliwiać odtwarzanie pojedynczych tabel dla minimum: Oracle, DB2, PostgreSQL, MySQL, Informix, MS SQL.
73. Automatyczny backup logów transakcyjnych dla baz danych w oparciu o procent wolnego miejsca na systemie plikowym, minimum dla: Oracle, SQL, Notes, SAP/Oracle.
74. Dla MS SQL możliwość skonfigurowania rozszerzenia pozwalającego backupować i odtwarzać bazy bezpośrednio z konsoli Management Studio.
75. Wsparcie dla backupu online dla minimum MS SQL Server 2016/2014/2012/2008/2005
76. Dedykowany agent bazodanowy dla backupu MS SQL na platformie Linux: Ubuntu, SuSe, RHEL.
77. Możliwość (jako opcja) archiwizacji danych z baz Oracle do plików XML.
78. Odtwarzanie baz SAP opartej na silniku Oracle do pliku, a więc odtwarzanie backupu online na dysk (tzw. application free restore).
79. Możliwość integracji kopii migawkowych dla backupu konsystentnego aplikacji i baz danych minimum: Vmware, Hyper-V, MS SQL, Exchange, mySQL, Oracle – zarządzanie kopiami

migawkowymi musi odbywać się z konsoli administracyjnej systemu backupowego a integracja zarządzania nie może odbywać się na bazie skryptów

80. Możliwość backupu i odtwarzania (jako opcja) dedykowanym agentem dokumentów i maili dla Office 365 z:
    1) SharePoint Online;
    2) Exchange Online;
    3) OneDrive;
    4) Teams.
81. Możliwość (jako opcja) pełnokontekstowego indeksowania i wyszukiwania treści z danych backupowanych (dokumenty i maile) z O365.
82. System musi zapewniać (jako opcja) backup laptopów i desktopów – funkcjonalność ta musi być w pełni zintegrowana z systemem (ta sama konsola, to samo repozytorium danych, ta sama deduplikacja) o funkcjonalnościach:
    1) Rozwiązanie musi pozwalać na archiwizację danych z możliwością pozostawiania znaczników (stub) na zasobach produkcyjnych (dla zasobów plikowych Windows\Linux\Unix) serwerów fizycznych, archiwizacja musi korzystać z tej samej architektury systemu co backup i korzystać z tego samego repozytorium danych;
    2) System musi posiadać funkcjonalności archiwizacyjne (archiwizacja plikowa);
    3) System musi oferować mechanizm składowania kopii backupowych (retencja danych) oparty o czas i cykle. Oznacza to iż kopia backupowa jest przechowywana w repozytorium przez określony czas (np. tydzień, miesiąc, rok) a jej automatyczne skasowanie jest wykonane jeśli spełniony jest jednocześnie warunek ilości cykli a więc ilość backupów typu pełnego lub backupów syntetycznych znajdujących się w systemie;
    4) System musi oferować integrację z mechanizmami deduplikacyjnymi urządzeń typu appliance minimalne wsparcie to Catalyst i urządzenie StoreOnce. Integracja z StoreOnce musi być dostępna nie tylko dla Windows ale także dla Unix i Linux; 5) System (jako opcja) musi oferować rozbudowę o funkcjonalność przeszukiwania i analizy zasobów plikowych dla maszyn wirtualnych (minimum Vmware) całość działać związanych musi odbywać się na kopiach backupowych maszyn wirtualnych a nie na środowisku produkcyjnym;
    6) Musi istnieć możliwość zarządzania systemem poprzez Windows PowerShell;
    7) Wsparcie (jako opcja) dla replikacji maszyn wirtualnych Vmware z wykorzystaniem VIAO (VSphere APIs for I/O);
    8) Monitorowanie i alertowanie klientów systemu którzy są trybie offline, a więc komunikacja z nimi przez system backupowy nie jest możliwa.

Wymogi dla licencjonowania.

1. Niedopuszczalne jest aby licencjonowanie było zależne od ilości składowanych danych (kopii backupowych) na dowolnych nośnikach (np. dysk, taśma VTL czy to z deduplikacją czy bez.
2. Niedopuszczalne jest aby licencjonowanie było zależne od ilości komponentów środowiska backupowego, które będą wykorzystywane w procesie backupu czy odtwarzania danych.
3. Zaoferowane licencje nie mogą ograniczać wielkości przestrzeni do składowania danych czy replik ich do innych lokalizacji. Jakakolwiek rozbudowa przestrzeni dyskowej czy to w siedzibie podstawowej czy innej nie może wymagać zakupu jakichkolwiek licencji dla systemu.
4. Oferowana licencja oraz architektura systemu musi pozwalać na backup danych na:
    1) nielimitowaną ilość bibliotek taśmowych i napędów fizycznych;
    2) nielimitowaną przestrzeń w rozwiązaniach chmurowych (minimum: AWS, Azure, Google).
5. W przypadku wielu lokalizacji licencja musi pozwalać na nielimitowaną replikację danych po deduplikacji pomiędzy lokalizacjami.
6. Do dostarczonych licencji jest wymagane 60-miesięczne wparcie producenta (pierwsza i druga linia wsparcia świadczona w języku polskim) zapewniające wsparcie techniczne w trybie dni roboczych oraz dostęp do bezpłatnych ewentualnych poprawek i uaktualnień. Oferowane wsparcie serwisowe musi być świadczone przez producenta rozwiązania lub autoryzowanego partnera serwisowego producenta na terenie Polski. W przypadku serwisu świadczonego przez autoryzowanego partnera serwisowego producenta na terenie Polski wymagane jest

potwierdzenie jakości świadczonych usług poprzez certyfikat ISO 9001:2015 na świadczone usługi serwisowe.

7. Zaoferowane licencje na system muszą zapewnić backup danych z środowiska o wielkości:
- środowisko maszyn wirtualnych wraz z aplikacjami i bazami – 1 maszyna wirtualna
- środowisko komputerów stacjonarnych – 30 stanowisk komputerowych

Wdrożenie systemu składowania i archiwizacji danych oraz wykonywania kopii zapasowych
Specyfikacja

Wdrożenie obejmie:

a) Instalacja urządzenia typu NAS oraz konfiguracja obejmująca m.in.:
   - instalacja systemu
   - dysków oraz ich trybu pracy RAID
   - podłączenie do istniejącej sieci
   - ustanowienie uprawnień zasobów oraz użytkowników
   - zabezpieczenie zasobów

b) Instalacja oraz konfiguracja systemu kopii bezpieczeństwa obejmującego m.in.:
   - serwer pracujący w środowisku zwirtualizowanym
   - stacje robocze

4. Rozbudowa i modernizacja sieci LAN

Przełącznik sieciowy w liczbie 1 sztuk oraz jego montaż i konfiguracja.
Specyfikacja

1. Parametry fizyczne platformy:
   - wymiary urządzenia powinny pozwalać na montaż w szafie rack 19", obudowa nie powinna być wyższa niż 1U
   - Zasilanie 230V
   - MTBF > 10lat

2. Interfejsy sieciowe – wymagania minimalne:
   - 48 portów GE, RJ-45
   - 4 porty 10GE SFP+

3. Zarządzanie:
   - port konsoli szeregowej RJ45
   - Zarządzanie przez wiersz poleceń (SSH) oraz poprzez graficzny interfejs poprzez przeglądarkę
   - Możliwość zarządzania poprzez kontroler przełączników pozwalający na automatyczne wykrywanie i centralne konfigurowanie przełączników oraz będący jednocześnie konsolą do zarządzania rozwiązaniami NGFW (Next Generation Firewall)
   - Kontroler przełączników musi być w stanie wykonywać pewne akcje automatycznie, bez ingerencji administratora a pod wpływem rozpoznanej topologii – m.in. automatyczna konfiguracja Spanning Tree, tagowanie 802.1q, automatyczne przejęcie zarządzania nad wykrytym przełącznikiem.
   - Kontroler przełączników musi umożliwiać aktualizację oprogramowania zarządzanych przełączników
   - Z poziomu kontrolera musi być możliwość podejrzenia informacji o typie urządzeń wykrytych na wybranym porcie przełącznika (np. system Linux, Windows itp.).
   - Kontroler musi oferować możliwość automatycznej instalacji wskazanej wersji oprogramowania układowego firmware, po podłączeniu przełącznika. Oprogramowanie przełącznika, musi być przechowywane na kontrolerze.

4. Parametry wydajnościowe:
   - przepustowość urządzenia - min. 176 Gbps, min. 260 Mpps

- możliwość zapamiętania co najmniej 32 000 adresów MAC
- Opóźnienie - poniżej 1 mikrosekundy
- Bufor pakietów: min. 2 MB
- Pamięć DRAM: min. 512 MB
- Pamięć FLASH: min. 64 MB

5. Wymagane funkcje:
   - możliwość automatycznej negocjacji prędkości i duplexu dla połączeń
   - obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree)
   - możliwość agregacji portów zgodna z 802.3ad
   - obsługa co najmniej 4000 VLANów, zgodna z 802.1Q
   - możliwość wykonywania routingu statycznego (realizowany software'owo)
   - port-mirroring
   - Kontrola dostępu na poziomie portu w oparciu o standard 802.1x, możliwość uwierzytelniania w oparciu o bazę Radius
   - zarządzanie przy użyciu Telnet/SSH, HTTP/HTTPS, SNMP w wersjach 1-3, SNTP, LLDP (w trybie odbioru)
   - możliwość zarządzania przez interfejs graficzny i tekstowy
   - możliwość aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI
   - możliwość integracji z systemem bezpieczeństwa NGFW, w zakresie co najmniej:
     - możliwość uruchomienia Captive Portalu w celu identyfikacji użytkowników
     - obsługa białych i czarnych list MAC
     - stateful firewall, umożliwiający kontrolę dostępu do sieci
     - routing statyczny i dynamiczny, co najmniej OSPF

6. Gwarancja oraz wsparcie:

   - Wsparcie serwisowe: System powinien być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, wymagane jest posiadanie dokumentu producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej.