Załącznik nr 1 do SWZ (RIiD.271.5.2023)

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

SPIS TREŚCI

1. Wprowadzenie

1.1. Niniejszy dokument jest Opisem Przedmiotu Zamówienia dotyczącym infrastruktury technicznej, zamawianej przez Gminę Gnojnik. Zamówienie realizowane jest w ramach grantu „Cyfrowa Gmina".

1.2. **Cyfrowa Gmina** projekt w ramach Działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia

1.3. **Węzeł centralny** – Centrum przetwarzania danych, zlokalizowane u Zamawiającego

1.4. **Zamawiający** – Urząd Gminy Gnojnik

1.5. **Wykonawca** – podmiot wybrany przez Zamawiającego do realizacji niniejszego zamówienia.

1.6. **Użytkownik systemu** – pracownik lub współpracownik Zamawiającego, pracownik jednostki organizacyjnej lub budżetowej Zamawiającego. Przez określenie „współpracownik" należy rozumieć osobę fizyczną, która nie jest zatrudniona u Zamawiającego na umowę o pracę, ale współpracuje z nim na zasadzie umowy zlecenia lub umowy o dzieło;

1.7. Pozostałe określenia użyte w opracowaniu należy rozumieć zgodnie z powszechnie akceptowaną nomenklaturą w dziedzinie problematyki objętej Zamówieniem.

2. Opis rozwiązania

2.1. Stworzenie bezpiecznego środowiska przetwarzania danych – Węzła Centralnego

2.1.1. Podstawowym założeniem niniejszego punktu jest utworzenie zduplikowanego środowiska węzła centralnego, pracującego w trybie active-active.

2.1.2. Zamawiający zamierza uruchomić zamawiany sprzęt i oprogramowanie w jednej lokalizacji.

2.1.3. Zamawiający planuje przygotować w przyszłości, pomieszczenia w drugiej lokalizacji oddalonej od bazowej lokalizacji o ok. 1000 m i oczekuje, że dostarczone urządzenia (wkładki światłowodowe), zapewnią połączenia na takiej odległości (przenosząc część sprzętu z obecnej lokalizacji do nowopowstałej).

2.1.4. Planowane jest utworzenie dwóch niezależnych centrów przetwarzania danych, umownie nazwanych „Serwer 1" i „Serwer 2".

2.1.5. Każde z ww. centrów będzie wykorzystywało własne zasoby dyskowe.

2.1.6. W każdym środowisku, planowane jest uruchomienie oprogramowania do wirtualizacji, obejmującego po 1 serwerze fizycznym.

2.1.7. Oprogramowanie do wirtualizacji będzie miało funkcjonalność, umożliwiającą replikację wybranych zasobów dyskowych z jednego środowiska fizycznego do drugiego, dzięki czemu Zamawiający będzie w stanie samodzielnie zdecydować, które krytyczne zasoby będą podlegały replikacji do środowiska przeciwnego i w jakich odstępach czasowych. Rozwiązanie takie umożliwi Zamawiającemu odtworzenie krytycznych systemów w środowisku przeciwnym, w przypadku krytycznej, długotrwałej awarii w lokalizacji podstawowej (tzw. Disaster Recovery).

2.1.8. Wraz z oprogramowaniem do wirtualizacji planowany jest zakup programów, tego samego producenta, które ułatwią Zamawiającemu i zautomatyzują przywracanie do pracy systemów biznesowych w środowisku zapasowym, dzięki czemu przerwa w pracy tych systemów zostanie zmniejszona do niezbędnego minimum.

2.1.9. Środowisko kopii zapasowej będzie przygotowane na bazie serwera Dell R420 będącego w posiadaniu przez zamawiającego (2 procesory 4 rdzeniowe, 16 GB RAM, 4x4TB HDD SAS, 2x 1Gbit Ethernet).

2.2. Zbiorcze zestawienie zamawianego sprzętu i oprogramowania

L.p.	Nazwa	Ilość	Nr tabeli
1.	Serwer RACK	2	4.1
2.	Zasilacz awaryjny	1	4.2
3.	Oprogramowanie do wirtualizacji[1)]	1	4.3
4.	Oprogramowanie do realizacji usług katalogowych[2)]	1	5.3
5.	Oprogramowanie do serwera kopii zapasowej	1	6.3
6.	Elementy uzupełniające	1 komplet	7.3

Uwagi do tabeli:

1) W tabeli wyspecyfikowano jedną sztukę oprogramowania do wirtualizacji, jako że ma to być spójny, jednolity system umożliwiający przenoszenie serwerów wirtualnych pomiędzy dwoma lokalizacjami w przypadku awarii lokalizacji podstawowej. Niemniej jednak, jak wyspecyfikowano dalej, oczekuje się dostarczenia rozwiązania, które umożliwi niezależne zarządzanie wirtualizacją w „Serwer 1" i w „Serwer 2".

2) Oprogramowanie do realizacji usług katalogowych w postaci Serwerowego Systemu operacyjnego (SSO) ma umożliwiać stworzenie dwóch serwerów usług katalogowych (podstawowy i zapasowy), oraz posiadać odpowiednie licencje dostępowe dla wyspecyfikowanej ilości klientów.

2.3. Wymagane usługi instalacyjno-wdrożeniowe

2.3.1. W ramach całego, niniejszego projektu wymaga się, aby Wykonawca dostarczył i zainstalował opisany w tym dokumencie sprzęt do lokalizacji opisanej w pkt. 3.1.1

2.3.2. W celu utworzenia środowiska Wykonawca:

2.3.2.1 Zainstaluje i skonfiguruje oprogramowanie do wirtualizacji, osobno dla „Serwer 1" i „Serwer 2". Przed rozpoczęciem prac, Wykonawca ustali z Zamawiającym sposób bootowania serwerów (czy z macierzy dyskowej, czy z pamięci Flash/SSD znajdującej się w każdym z serwerów);

2.3.2.2 Zainstaluje i skonfiguruje w środowisku wirtualnym w „Serwer 1", oprogramowanie do obsługi usług katalogowych.

2.3.2.3 Uruchomi replikację ww. serwerów wirtualnych (ich zasobów dyskowych) do środowiska wirtualnego w „Serwer 2".

2.3.2.4 Założy i skonfiguruje w usłudze katalogowej konto dla przykładowego użytkownika.

2.3.2.5 Tak skonfiguruje komputer przykładowego użytkownika oraz urządzenia sieci komputerowej (przełączniki Ethernet, UTM, itp.), aby logowanie do sieci wymagało od tego użytkownika podania loginu i hasła.

2.3.2.6 Zasymuluje awarię całego środowiska wirtualnego w „Serwer 1" i odtworzy w „Serwer 2" oprogramowanie do obsługi usług katalogowych, na podstawie zapisanych tam replik zasobów dyskowych.

2.3.2.7 Sprawdzi możliwość logowania się do sieci przykładowego użytkownika na komputerze wskazanym przez Zamawiającego.

2.3.2.8 Skonfiguruje usługę RDP, w szczególności brokera RDP i galerii programów RDP.

2.3.2.9 Wykona migracja posiadanych systemów (PortalInteresanta, SIDAS, IPmapa) na nowo wdrożone serwery oraz wdrożenie kontenerowych rozwiązań dla następujących środowisk bazodanowych:

2.3.2.9.1 5 środowisk (instancji) bazodanowe MS SQL

2.3.2.9.2 2 środowiska bazodanowe PostgreSQL

2.3.2.9.3 2 środowiska bazodanowe FirebirdSQL

2.3.2.10 Skonfiguruje połączenie „Serwer 2" z UPS-em zakupionym w tym postępowaniu oraz w przypadku zaniku prądu gdy stan naładowania baterii UPS spadnie do poziom 50% wyłączy wszystkie maszyny wirtualne uruchomione na „Serwer 2" oraz wyłączy cały serwer.

2.3.2.11 Skonfiguruje port do zdalnego zarządzania serwerem (wyspecyfikowany w pkt 4.1.13 c) dla każdego z zakupionych serwerów.

2.3.2.12 Wykona usługi opisane w dalszej części dokumentu, przy poszczególnych urządzeniach i oprogramowaniu.

3. Środowisko instalacji i wdrożenia

3.1. Środowisko instalacji i wdrożenia węzła centralnego u Zamawiającego

3.1.1. Sprzęt i oprogramowanie dostarczane będzie w lokalizacji Zamawiającego:

a) siedziba Zamawiającego w Gnojniku, 32-864 Gnojnik 363

3.1.2. Zamawiający dysponuje klimatyzowaną serwerownią i miejscem w szafach RACK umożliwiającym zainstalowanie zamawianego sprzętu.

3.1.3. Serwerownia ulokowane są na drugim piętrze budynku, z szerokimi schodami.

3.1.4. Wszystkie prace niewymagające przerwy w pracy pracowników Zamawiającego mogą być realizowane w godzinach od 8 do 16 od poniedziałku do piątku.

3.1.5. Prace wymagające przerwy w pracy pracowników Zamawiającego mogą być realizowane po wcześniejszym uzgodnieniu z Zamawiającym, poza godzinami pracy Zamawiającego, które na dzień ogłaszania przetargu są następujące:

a) 7:30 - 16:30 – poniedziałek
b) 7:30 - 15:30 – od wtorku do czwartku
c) 7:30 - 14:30 – piątek

3.1.6. Dostarczone rozwiązanie zastąpi część urządzeń obecnie funkcjonujących u Zamawiającego, w związku z tym Wykonawca będzie musiał dostosować ich konfigurację (np. adresację IP) do rozwiązań obecnie stosowanych przez Zamawiającego. Oczekuje się, że przed wdrożeniem całego systemu Wykonawca zapozna się z konfiguracją urządzeń (np. UTM, przełączniki LAN itp.) funkcjonującą u Zamawiającego.

3.1.7. Zamawiający wykorzystuje techniki zabezpieczające: firewalle, NAT, VPN, antywirusy, antyspam itp.

4. Wyposażenia serwerowni – Węzeł centralny

4.1. **Serwer – sztuk 2**		
	Wymagania funkcjonalno-techniczne	
1.	Obudowa	Umożliwiająca instalację w standardowej szafie RACK 19”.
2.	Płyta główna	Płyta główna z możliwością zainstalowania przynajmniej dwóch procesorów wykonujących 64-bitowe instrukcje AMD64 lub EM64T (np. AMD albo Intel).
3.	Procesor	Procesor 16-rdzeniowy 32 wątkowy, osiągający w oferowanym serwerze wynik przynajmniej 235 pkt. w konfiguracji dwuprocesorowej w teście CPU2017 Floating Point Rates. Wymagana jest obecność protokołu potwierdzającego osiągnięty wynik na stronie: www.spec.org (wydruk ze strony należy dołączyć do oferty).
4.	Liczba procesorów	2 szt.
5.	Pamięć RAM	min. 128 GB. Ilość wolnych slotów dla pamięci RAM musi umożliwiać jej rozbudowę do min. 512 GB, w modułach takich jak podstawowe 128 GB.
6.	Dyski SSD	min. 4 szt. dysków NVMe 1,9 TB 2,5”. Serwer musi umożliwiać rozbudowę w przyszłości przestrzeni dyskowej o kolejne 4 dyski (łącznie musi mieć możliwość zainstalowania 8-miu dysków).
7.	Pamięć nieulotna SD/FLASH	Serwer musi mieć możliwość instalacji pamięci nieulotnej SD lub FLASH o wielkości min. 64 GB, umożliwiającą zainstalowanie oprogramowania do wirtualizacji (hypervisor) i bootowanie z niej serwera.
8.	Dyski szybkiego startu	min. 2 dyski 240 GB SSD M.2 z osobnym kontrolerem RAID1
9.	Napęd	DVD-RW
10.	Interfejsy sieciowe	2 szt. 10/100/1000 Mbit/s Ethernet
11.	Kontroler RAID	a) min. 8 GB Cache, b) transfer 12 Gbit/s, c) rodzaje dysków: NVMe d) RAID poziomu: 1, 5, 6, 10, 50, 60 e) wspierane systemy: Linux, Windows Server, VMWare
12.	Karta SFP+	2 szt. 10 Gbit/s – światłowodowe SFP+
13.	Dodatkowe sloty / porty	a) PCIe 4.0 – min. 1 szt. Slot musi być nieobsadzony (niezajęty) przez inne karty (np. kontroler RAID), umożliwiając ich przyszłe wykorzystanie przez Zamawiającego. b) VGA. c) Port do zdalnego zarządzania serwerem – niezależny od 2 portów

		Ethernet wyspecyfikowanych w pkt. 10. Port zdalnego zarządzania musi posiadać funkcjonalność wirtualnego KVM-a z możliwości uruchomienia konsoli serwera w technologii HTML5
14.	Zasilanie	2 szt. zasilaczy min. 600W umożliwiających zasilanie serwera z dwóch niezależnych obwodów zasilających i poprawną pracę serwera podczas zaniku napięcia w jednym z obwodów lub przy awarii jednego z zasilaczy. Możliwość wymiany uszkodzonego zasilacza, bez konieczności wyłączania całego serwera (hot-swap).
15.	Chłodzenie	Min. 6 szt. wentylatorów.
16.	Szyny montażowe	Szyny ruchome
17.	Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
18.	Gwarancja	Gwarancją producenta na następny dzień roboczy min. 3 lata. Zachowanie dysków twardych min. 3 lata

4.2. Zasilacz awaryjny (UPS) – sztuk 1

	Wymagania funkcjonalno-techniczne	
1.	Obudowa	Umożliwiająca instalację w standardowej szafie RACK 19”.
2.	Moc	Minimum 2000 VA / 1800W. Zamawiający oczekuje, iż czas podtrzymania UPS-a nie będzie krótszy niż 6 min. przy 70% obciążeniu.
3.	Sposób działania	On-line z podwójną konwersją.
4.	Znamionowe napięcie wejściowe	230 V
5.	Znamionowe napięcie wyjściowe	230 V
6.	Ilość gniazd sieciowych	Min. 8 szt. IEC C13
7.	Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.

4.3. Oprogramowanie do wirtualizacji

	Wymagania funkcjonalno-techniczne
1.	System do wirtualizacji musi umożliwić stworzenie dwóch środowisk logicznych, wykorzystujących osobne zasoby serwerowe (Serwer 1” i „Serwer 2). Obydwa środowiska będą osobno zarządzane, z dedykowanej dla każdego środowiska konsoli zarządzającej.
2.	System musi być zainstalowany bezpośrednio na sprzęcie fizycznym, bez konieczności instalacji dodatkowego systemu operacyjnego. Rozwiązanie musi być niezależne od producenta platformy sprzętowej, tzn. nie może wskazywać tylko jednego producenta sprzętu.
3.	System musi umożliwić uruchomienie wielu instancji systemów operacyjnych na jednym serwerze fizycznym. Przy czym wspierane muszą być przynajmniej następujące systemy operacyjne: a. Windows Server w wersji co najmniej 2019 i 2022. b. Suse Linux Enterprise Server w wersji 10 i nowszej, c. Red Hat Enterprise Linux w wersji 5 i nowszej.
4.	System musi umożliwiać zastosowanie w serwerach fizycznych, procesorów o dowolnej ilości rdzeni oraz zapewnić możliwość przydzielenia maszynom wirtualnym do 128 procesorów wirtualnych.
5.	System musi umożliwiać przydzielenie maszynom wirtualnym, łącznie większej przestrzeni dyskowej niż jest fizycznie dostępna w zasobach dyskowych.
6.	System musi posiadać możliwość sprzętowego wsparcia dla wirtualizacji zagnieżdżonej.

7.	System dla każdego środowiska osobno („Serwer 1" i „Serwer 2"), musi posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i usługami, w tym możliwość monitorowania wykorzystania zasobów fizycznych, infrastruktury wirtualnej.
8.	Konsola do zarządzania środowiskiem wirtualnym musi pochodzić od tego samego producenta co sam system do wirtualizacji, tak aby Zamawiający nie był zmuszony do szkolenia pracowników u dwóch różnych (lub więcej) producentów. Awaria pojedynczego serwera nie może blokować dostępu do konsoli zarządzania
9.	Dostęp przez przeglądarkę do graficznej konsoli zarządzania musi być skalowalny tj. powinien umożliwiać rozdzielenie komponentów na wiele instancji, w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska.
10.	System musi zapewniać możliwość wykonywania kopii migawkowych serwerów wirtualnych i instancji systemów operacyjnych, na potrzeby tworzenia kopii zapasowych (bez przerywania pracy tych systemów i serwerów wirtualnych).
11.	System musi umożliwiać tworzenie replik obrazów dyskowych maszyn wirtualnych uruchomionych w środowisku „Serwer 1" na macierz dyskową zainstalowaną w „Serwer 2" i odwrotnie. System musi umożliwiać określenia częstotliwości wykonywania ww. kopii zasobów dyskowych.
12.	System musi umożliwiać tworzenie klastrów z serwerów fizycznych, w celu zapewnienia wysokiej dostępności maszyn wirtualnych i aplikacji (high availability).
13.	System musi posiadać możliwość przydzielania i konfiguracji uprawnień użytkownikom poprzez integrację z usługami katalogowymi (np. Microsoft Active Directory. LDAP itp.).
14.	System musi pozwalać na tworzenie wirtualnych przełączników LAN, obsługę sieci vLAN – Zarządzanie przełącznikami wirtualnymi powinno odbywać się z centralnej konsoli opisanej w pkt. 8.
15.	System musi zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi.
16.	Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii zapasowych instancji systemów operacyjnych oraz ich odtworzenia w możliwie najkrótszym czasie.
17.	Kopie zapasowe muszą być składowane z wykorzystaniem technik de-duplikacji danych.
18.	Musi istnieć możliwość odtworzenia pojedynczych plików z kopii zapasowej maszyny wirtualnej przez osoby do tego upoważnione, bez konieczności nadawania takim osobom bezpośredniego dostępu do głównej konsoli zarządzającej całym środowiskiem.
19.	Mechanizm zapewniający kopie zapasowe musi być wyposażony w system cyklicznej kontroli integralności danych. Ponadto musi istnieć możliwość przywrócenia stanu kopii zapasowych do punktu w czasie, kiedy wszystkie dane były integralne w przypadku awarii tego repozytorium.
20.	Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
21.	Rozwiązanie musi zapewniać mechanizm bezpiecznego, bezprzerwowego i automatycznego uaktualniania warstwy wirtualizacyjnej, wliczając w to zarówno poprawki bezpieczeństwa jak i zmianę jej wersji.
22.	Rozwiązanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci.
23.	Decyzja o próbie przywrócenia funkcjonalności maszyny wirtualnej w przypadku awarii lub niedostępności serwera fizycznego powinna być podejmowana automatycznie przez system, jednak musi istnieć możliwość określenia przez administratora czasu po jakim taka decyzja jest wykonywana.
24.	Dla każdego środowiska wirtualnego („Serwer 1" i „Serwer 2") wymagane jest oprogramowanie pochodzące od tego samego producenta co sam system do wirtualizacji, które w przypadku poważnej awarii (katastrofy) jednego z centrów danych, zautomatyzuje i przyspieszy uruchomienie krytycznych systemów użytkownych w drugim środkowisku. Oprogramowanie to: a. Będzie wykorzystywało repliki (kopie) obrazów dyskowych, wykonywanych przez system do wirtualizacji – patrz punkty 10 i 11 w niniejszej tabeli; b. Umożliwi tworzenie grup serwerów wirtualnych, które powinny być odtwarzane razem (np. dla systemu obiegu dokumentów: serwer bazodanowy, serwer aplikacyjny i serwer WWW);

	c. Umożliwi przygotowanie skryptów, określających w jakiej kolejności, jakie zasoby należy zwolnić w lokalizacji zapasowej (np. wyłączyć pewne serwery wirtualne) i jakie uruchomić z kopii, aby przywrócić do pracy najbardziej krytyczne systemy użytkowe; d. Umożliwi przygotowywanie ww. skryptów w tej samej konsoli zarządzającej, co cały system do wirtualizacji; e. Umożliwi przeprowadzanie testów odtworzeniowych, w odizolowanym środowisku sieciowym, tak aby przy normalnej pracy systemów użytkowych (bez konieczności ich wyłączania), móc zweryfikować, czy ich odtworzenie w lokalizacji zapasowej będzie możliwe w sytuacji awaryjnej; f. Uprości i przyspieszy przywrócenie systemów użytkownych do pracy po awarii (Failback) w ich oryginalnych lokalizacjach, poprzez wykonanie przygotowanych wcześniej planów awaryjnych w odwrotnej kolejności;	
25.	Licencje i wsparcie techniczne	W cenie systemu do wirtualizacji musi być dostarczona licencja: a. Uprawniająca do uruchomienie dowolnej ilości serwerów wirtualnych, b. Nie posiadająca żadnego ograniczenia czasowego ani jeśli chodzi o ważność licencji, ani jeśli chodzi o termin użytkowania oprogramowania, c. Uprawniająca do niezależnego zarządzania środowiskiem „Serwer 1” i środowiskiem w „Serwer 2”,

5. Zarządzania bezpieczeństwem sieci – domena

5.1. Cel zadania

Celem niniejszego zadania jest:

5.1.1. Przyspieszenie nadawania i odbierania uprawnień użytkownikom pracującym w sieci komputerowej, a w szczególności przydzielania i odbierania uprawnień do systemów przetwarzających dane osobowe.

5.1.2. Pomoc administratorom sieci komputerowej i poszczególnych systemów informatycznych w nadzorze nad pracą użytkowników, w tym ograniczenie tym użytkownikom dostępu do nośników danych, które mogą być źródłem wycieku danych osobowych.

5.1.3. Monitoring sieci komputerowej, ułatwiający i przyspieszający identyfikowanie awarii i zagrożeń pojawiających się w sieci.

5.2. Oczekiwane rozwiązanie

Zakłada się realizację celu opisanego w punkcie 5.1, w następujący sposób:

5.2.1. Nadawanie, ograniczanie i odbieranie uprawnień użytkownikom pracującym w sieci komputerowej planuje się wykonać poprzez zakup i uruchomienie systemu realizującego usługi katalogowe, takie jak np. LDAP lub Active Directory. Wszystkie lub większość systemów będą wykorzystywały tę usługę przynajmniej do autentykacji użytkowników. Dzięki temu odebranie uprawnień użytkownikowi (zablokowanie jego konta) w usłudze katalogowej, powinno skutkować automatycznym pozbawieniem dostępu do innych systemów dziedzinowych, w tym do tych, które przetwarzają dane osobowe.

5.3. **Oprogramowanie do realizacji usług katalogowych w oparciu o Serwerowy System Operacyjny (SSO)**	
	Wymagania funkcjonalno-techniczne

1.	Ilość i rodzaj licencji	Dostarczone licencje dla oprogramowania Serwerowego Systemu Operacyjnego (SSO) realizującego usługę katalogową nie mogą posiadać żadnego ograniczenia czasowego ani jeśli chodzi o ważność licencji, ani jeśli chodzi o termin użytkowania oprogramowania, ani powiązanie ze sprzętem, na którym będą użytkowane (nie może to być licencja typu OEM), a ponadto muszą: a. Uprawniać do instalacji w środowisku wirtualnym uruchomionym na serwerze „Serwer1" opisanym powyżej, b. Umożliwić zarządzanie poprzez usługę katalogową min. 50 urządzeniami niezależnie od ilości użytkowników. c. Dodatkowo planuje się wykorzystać pracę terminalową przez 5-ciu użytkowników.
2.	SSO musi obsługiwać wolumeny umożliwiające: a. zmianę rozmiaru w czasie pracy systemu, b. tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c. kompresję "w locie" dla wybranych plików i/lub folderów, d. zdefiniowanie list kontroli dostępu (ACL).	
3.	SSO musi udostępniać usługi katalogowe zgodne z LDAP i pozwalające na uwierzytelnianie użytkowników, bez konieczności instalowania dodatkowego oprogramowania na stacjach roboczych tych użytkowników.	
4.	Usługi katalogowe obsługiwane przez SSO muszą umożliwiać zarządzanie zasobami w sieci (użytkownikami, komputerami, drukarkami, udziałami sieciowymi itp.), z możliwością wykorzystania następujących funkcji: a. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, b. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, c. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.	
5.	SSO i usługi katalogowe musi mieć możliwość definiowania polityk, które przy zalogowaniu użytkownika do sieci umożliwią ograniczenie jego dostępu do urządzeń dostępnych na jego stacji roboczej (np. pozbawienie dostępu do portów USB komputera).	
6.	SSO powinien umożliwiać zdalną dystrybucję oprogramowania na stacje robocze.	
7.	SSO musi mieć możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO, umożliwiającego lokalną dystrybucję poprawek, zatwierdzonych przez administratora, bez połączenia z siecią Internet.	
8.	SSO musi mieć, pochodzący od producenta systemu, serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).	
9.	SSO musi umożliwiać automatyczną weryfikację cyfrowych sygnatur sterowników, w celu sprawdzenia, czy sterownik przeszedł testy jakości, przeprowadzone przez producenta systemu operacyjnego.	
10.	SSO musi umożliwiać szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.	
11.	SSO musi umożliwiać szyfrowanie plików i folderów.	
12.	SSO musi posiadać wbudowaną zaporę internetową (firewall), z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.	
13.	SSO musi umożliwiać szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).	
14.	SSO powinien mieć wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.	
15.	SSO powinien obsługiwać Centrum Certyfikatów (CA) umożliwiające: a. Dystrybucję certyfikatów poprzez http	

	b. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen.
16.	SSO musi umożliwiać uruchamianie aplikacji wykorzystujących technologię ASP.NET.
17.	SSO musi mieć wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
18.	SSO musi mieć graficzny interfejs użytkownika.
19.	SSO musi być w języku polskim, co najmniej jeśli chodzi o następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
20.	SSO musi mieć możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
21.	SSO musi mieć możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management.
22.	SSO musi mieć dostęp do bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23.	SSO powinien mieć możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
24.	SSO musi mieć możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów, wymagających dodatkowych licencji: DHCP oraz DNS wspierający DNSSEC.

6. Środowisko kopii zapasowej

6.1. Cel zadania

Celem niniejszego zadania jest uruchomienie i skonfigurowanie systemu zabezpieczenia danych Węzła centralnego.

6.2. Oczekiwane rozwiązanie

Zakłada się realizację celu opisanego w punkcie 6.1, w następujący sposób:

6.2.1. W zakresie uruchomienia i skonfigurowania systemu zabezpieczenia danych, planuje się zakupić oprogramowanie umożliwiające wykonywanie automatycznych kopii zapasowych całego środowiska wirtualnego w systemie „disk-to-disk”. Podstawowym warunkiem stawianym całemu rozwiązaniu jest możliwość:

a) wykonywania kopii bez konieczności zatrzymywania jakiegokolwiek elementu całego systemu (środowiska wirtualnego, serwerów wirtualnych, baz danych, systemów dziedzinowych, czy aplikacji użytkowników);
b) odtworzenie poszczególnych serwerów wirtualnych w sposób zapewniający spójność danych;
c) odtworzenie poszczególnych plików w obrębie pojedynczego serwera wirtualnego;
d) odtworzenie poszczególnych baz danych SQL, zachowując ich spójność.

6.2.2. Wykonanie punktów 6.2.1 a) do d) na działającym i skonfigurowanym „Węźle Centralnym” będzie wymogiem podpisania protokół odbioru przedmiotu umowy.

6.2.3. Na bazie serwera będącego w posiadaniu przez Zamawiającego zostanie skonfigurowane środowisko kopii zapasowych tego samego producenta co Oprogramowanie do wirtualizacji wymienione w punkcie 4.3 z następującymi wymaganiami:

6.3. **Konfiguracja Serwer do backupu**		
	Wymagania funkcjonalno-techniczne	
1.	Środowisko fizyczne: Serwer wskazany przez Zamawiającego: Dell R420 (8 rdzeni, 16GB RAM, 4 x4TB HDD SAS, 2x 1GBbit/s Ethernet	
2.	Wymagania w odniesienie do oprogramowania kopii zapasowej	Serwer wskazany (wyspecyfikowany) powyżej ma być wystarczający do uruchomienia oprogramowania serwera kopii zapasowej z następującej funkcjonalnościami (działającymi płynnie):
		Wykonywanie automatycznych kopii zapasowych całego środowiska wirtualnego.
		Wykonywania kopii zapasowych bez konieczności zatrzymywania jakiegokolwiek elementu całego systemu (środowiska wirtualnego, serwerów wirtualnych, baz danych, systemów dziedzinowych, czy aplikacji użytkowników).
		Możliwość odtworzenia całego środowiska wirtualnego (Disaster Recovery)
		Oprogramowanie musi współpracować z systemem wirtualizacyjnym opisanym w punkcie 4.3, m.in. poprzez wykorzystywanie snap-shotów wykonywanych przez ten system.
		Oprogramowanie musi mieć możliwość odtworzenia poszczególnych serwerów wirtualnych, kontenerów i fizycznych hostów w sposób zapewniający spójność danych.
		Możliwość odtworzenie pojedynczych plików w obrębie serwera wirtualnego, kontenera.
		Oprogramowanie powinno mieć wbudowane mechanizmy deduplikacji i kompresji, w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji.
		Oprogramowanie w przypadku konieczności instalacji wewnątrz maszyny wirtualnej agentów wymagających wdrożenia powinno być kompletne czyli dostarczone z agentami dla następujących najnowszych wersji systemów operacyjnych i silników bazodanowych: Windows Serwer lic. 5, Linux RedHat lic. 1, Linux Debian lic. 4, MS SQL Serwer lic.5, Firebird lic.2, PostgresSQL lic 2
		Oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP.
		Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.
		Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji.
		Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny.
		Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn z dowolnego backupu w izolowanym środowisku.
3.	Licencje	Dostarczone licencje muszą umożliwiać wykonywanie kopii zapasowych ze wszystkich serwerów fizycznych dostarczonych do stworzenia Węzła Centralnego oraz posiadanego serwera zakupionego w ramach postępowania CUW (serwer 2

		procesorowy)
		Licencja musi umożliwiać wykorzystanie wszystkich opisanych w niniejszym dokumencie funkcjonalności, bez konieczności dokupowania jakichkolwiek dodatkowych opcji.
		Licencja nie może posiadać żadnego ograniczenia czasowego ani jeśli chodzi o ważność licencji, ani jeśli chodzi o termin użytkowania oprogramowania.
		W sytuacji, gdy oprogramowanie do archiwizacji danych wymaga do poprawnego działania jakiegoś dodatkowego, licencjonowanego oprogramowania (np. systemu operacyjnego), to Wykonawca musi dostarczyć te licencje wraz z oprogramowaniem do archiwizacji danych.
4.	Aktualizacja	36 miesiące

7. Pozostałe wymagania

7.1. Wszelkie urządzenia i oprogramowanie dostarczone będzie w oryginalnych opakowaniach producenta, z dołączoną licencją, nośnikami i dokumentacją.

7.2. Dostarczone licencje będą wolne od roszczeń osób trzecich oraz bez możliwości ich wypowiedzenia w przypadku użytkowania oprogramowania zgodnie z licencją.

7.3. **Elementy uzupełniające**	
	Wymagania funkcjonalno-techniczne
1.	W ramach dostawy Wykonawca dostarczy komplet niezbędnego okablowania, patch-cordów, modułów, gniazd, listew zasilających, wtyczek itp. umożliwiających połączenie, uruchomienie i skonfigurowanie urządzeń i oprogramowania wymienionego w niniejszym dokumencie.