Załącznik nr 1 do SWZ

Niniejszy dokument określa szczegółowe wymagania dla zamówienia publicznego pn. **„Zakup, dostawa, instalacja i konfiguracja systemu do wykonywania kopii zapasowych i urządzenia klasy UTM w ramach projektu Cyberbezpieczny Samorząd”** na rzecz Gminy Wręczyca Wielka.

Zadanie realizowane jest w ramach projektu grantowego „Cyberbezpieczny Samorząd” dofinansowanego z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. „Wzmocnienie krajowego systemu cyberbezpieczeństwa”.

Przedmiot zamówienia obejmuje dostawę, instalację oraz konfigurację niżej wymienionych elementów:

Wymagania Szczegółowe Przedmiotu Zamówienia

I. Urządzenie do wykonywania kopii zapasowych

1. Zarządzanie i magazyny

1.1 Urządzenie wraz a aplikacją do wykonywania kopii zapasowej (SYSTEM) musi umożliwiać:

1.1.1 tworzenie kopii zapasowych na poziomie dysków,
1.1.2 tworzenie kopii zapasowych na poziomie plików i folderów,
1.1.3 replikację kopii zapasowych do wielu lokalizacji docelowych,
1.1.4 tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT,
1.1.5 współpracę z usługą kopiowania woluminów w tle (VSS) firmy Microsoft,
1.1.6 zdefiniowania limitu przepustowości sieciowej z jakiej ma korzystać oprogramowanie backupowe,
1.1.7 administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami,
1.1.8 wykonywanie kopii obrazu dysku, kopii plików i katalogów oraz kopii maszyn wirtualnych bez ich zatrzymywania z zachowaniem stuprocentowej integralności i spójności danych wewnątrz wykonanej kopii zapasowej,
1.1.9 automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku wystąpienia błędu,
1.1.10 mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle,
1.1.11 definiowanie tzw. okna backupowego dla każdego z zadań w celu umożliwienia zarządzania obciążeniem sieci i uwzględnienia okien serwisowych występujących u Zamawiającego,
1.1.12 automatyczne dodawanie do polityki i harmonogramu tworzenia backupów nowe źródła / maszyny wirtualnych, dodane do bieżącego środowiska (automatyzacja oparta na polityce tworzenia kopii),
1.1.13 zmniejszenie rozmiaru przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych,
1.1.14 automatyczne aktualizacje oprogramowania,
1.1.15 kompresowanie i szyfrowanie zabezpieczonych danych w systemach NAS,

1.1.16 uruchomienie kontenerów Docker w dowolnych urządzeniach NAS i innych środowiskach w celu ich zabezpieczenia,

1.1.17 gradację uprawnień administratorów - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: system operator, backup operator, restore operator, viewer. Dla każdej z tych ról system musi umożliwiać przypisywanie dodatkowych uprawnień, w tym możliwość zablokowania usuwania danych,

1.1.18 klonowanie planów kopii zapasowych, planów replikacji oraz planów testowego odtwarzania maszyn wirtualnych,

1.1.19 uruchamianie przy zadaniach backupu dowolnych skryptów PRE/POST oraz po wykonaniu migawki VSS,

1.1.20 wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika,

1.1.21 uruchomienie konsoli w chmurze producenta zlokalizowanej na terenie Polski, w celu umożliwienia dostępu do środowiska zarządzania kopiami zapasowymi w przypadku czasowej niedostępności środowiska lokalnego,

1.1.22 dostęp do konsoli administracyjnej z wielu stacji roboczych,

1.1.23 wyświetlenie szczegółowych informacji o chronionym urządzeniu takich jak: CPU, RAM, System operacyjny, Adres IP,

1.1.24 składowania utworzonych kopii zapasowych na magazynach chmurowych Amazon AWS, Azure, Wasabi, Google Cloud Storage, Backblaze B2, magazyny zgodne z S3 oraz dedykowana chmura producenta rozwiązania,

1.1.25 składowanie utworzonych kopii zapasowych na udziałach sieciowych po protokole smb, S3, nfs, iscsi, katalog lokalny,

1.1.26 tworzenie wielu repozytoriów danych jednocześnie również na innych środowiskach jako przestrzeń do replikacji danych,

1.1.27 generowanie raportów dobowych w oparciu o harmonogram.

1.2 System musi posiadać mechanizmy chroniące przejęcie konta administratora oraz umożliwiać definiowanie dodatkowych uprawnień dla każdej z predefiniowanych ról użytkowników.

1.3 System musi realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie.

1.4 System zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.

1.5 System musi udostępniać możliwość podglądu postępu działania dowolnego zadania, w tym zadania wykonywania kopii zapasowych, odtwarzania danych, testowego odtwarzania danych, usuwania danych oraz zadania odświeżania zajętości magazynu na dane.

1.6 System musi posiadać system powiadamiania poprzez min. e-mail o zdarzeniach w następujących przypadkach: zadanie zostało zakończone pomyślnie, zadanie zostało zakończone z ostrzeżeniami, zadanie zostało zakończone z błędem, zadanie zostało anulowane, zadanie nie zostało uruchomione.

1.7 Oferowane rozwiązanie musi być dobrane pod względem wydajności w oparciu o najlepsze praktyki producenta.

1.8 Rozwiązanie musi być wyskalowane, dobrane pod względem wymaganej funkcjonalności i wydajności stosownie do ilości zabezpieczanych danych i obiektów z uwzględnieniem przyrostu danych (serwery, maszyny wirtualne, bazy danych itp.) zgodnie z opisem w zapytaniu ofertowym.

1.9 Konfiguracja musi zapewniać pełną funkcjonalność systemu od momentu wdrożenia (np. deduplikacja, kompresja, workerzy i browsery, replikacja, testowe odtwarzanie maszyn wirtualnych).

1.10 System musi przechowywać dane w sposób zapewniający ich niezmienność, aby kopie zapasowe były chronione przed nadpisaniem lub modyfikacją przez cały okres retencji.

1.11 System musi przechowywać zaszyfrowane dane w kopii zapasowej i szyfruje ruch wewnętrzny.

1.12 System musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.

1.13 System musi posiadać możliwość zapisu kopii zapasowych do magazynu chmurowego dostarczanego bezpośrednio przez producenta oprogramowania (datacenter powinno być zlokalizowane na terenie Polski).

1.14 System musi posiadać możliwość zdefiniowania maksymalnej liczby równocześnie backupowanych urządzeń w ramach jednego planu backupowego, niezależnie od typu urządzenia (np. stacja robocza, serwer, maszyna wirtualna).

1.15 System musi posiadać możliwość zdefiniowania poziomu obciążenia magazynu, po osiągnięciu którego zostanie wysłane powiadomienia e-mail. (poziom definiowany indywidualnie dla każdego magazynu)

1.16 System musi posiadać możliwość nieodwracalnego usuwania danych z magazynu na dane w momencie spełnienia dodatkowych wymogów.

1.17 System musi zapewniać zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera (urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera (urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).

1.18 W sytuacji, gdyby podstawowe urządzenie tworzenia kopii zapasowej było niedostępne, system musi posiadać możliwość przywrócenia z archiwum za pomocą innej instancji systemu dostarczonej przez tego samego producenta. tzn. archiwum musi zawierać wszystkie informacje konieczne do odzyskania.

1.19 System powinien posiadać predefiniowane schemat tworzenia kopii zapasowych, min. Custom, Basic, G-F-S, Forever incremental,

1.20 Proces deduplikacji musi być możliwy dla każdego z typów obsługiwanych magazynów.

1.21 Proces deduplikacji nie może wymagać instalacji żadnych dodatkowych komponentów, które będą pośredniczyły w zapisie danych z deduplikowanych

1.22 Proces deduplikacji nie może posiadać pojedynczego punktu awarii, tym samym musi być dostępny jednocześnie na każdym wspieranym magazynie na dane - również replikacyjnych. Awaria jednego z magazynów na dane nie może wpłynąć na integralność deduplikatów, jak i tablicy deduplikatów na innym magazynie.

1.23 Proces deduplikacji realizowany jest blokiem o stałej wielkości, którego wielkość może zostać ustalona na etapie wdrożenia rozwiązania zgodnie z najlepszymi praktykami producenta.

1.24 Proces szyfrowania kopii zapasowych nie może ograniczać procesu deduplikacji w ramach tego samego klucza szyfrującego.

1.25 Kompresja kopii zapasowych musi obsługiwać jeden z wymienionych algorytmów: LZ4, ZStandard. Dodatkowo, musi umożliwiać określenie szczegółowego poziomu kompresji, w tym: niski, średni, wysoki.

1.26 Instalacja, modyfikacja ustawień, polityki tworzenia kopii zapasowej systemu nie może wymagać przerwania pracy lub restartu systemu.

1.27 Archiwum długoterminowych kopii zapasowych musi być szyfrowane, a odzyskiwanie z archiwum obsługiwane z tego samego interfejsu użytkownika, co inne przywracanie dane.

1.28 Rozwiązanie musi obsługiwać kontrolę dostępu opartą na rolach (RBAC).

1.29 Zarządzanie i odzyskiwanie danych z kopii musi odbywać się z tego samego interfejsu użytkownika (konsoli), niezależnie od tego, gdzie znajduje się kopia zapasowa (w chmurze AWS, Azure, GCP, w Data Center czy w usłudze typu SaaS).

1.30 Czas przechowywania kopii zapasowej (retention time) systemu backupu nie może być zmieniony np. poprzez manipulowanie wskazaniami zegara serwera NTP w celu szybszego ich wyekspirowania - tzn. czasy przechowywania kopii zapasowych nie będą zależne od wskazań zegara czasu serwera NTP, ale będą wykorzystywać technologię, która mierzy upływ czasu.

1.31 System zarządzania nie może być oparty o relacyjne bazy danych lub Zamawiający wymaga dostarczenia niezbędnych licencji zawartych w cenie urządzenia.

1.32 Rozwiązanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej).

1.33 System plików systemu musi być odporny na ataki Ransomware (zapewnić ochronę przed szyfrowaniem endto-end, kopie zapasowe nie mogą być nadpisywane - "niezmienny system plików").

1.34 System powinien umożliwiać wykorzystanie wbudowanego menadżera haseł do przechowywania wszelkich sekretów (haseł, danych dostępowych, kluczy szyfrujących) wykorzystywanych przez System

1.35 System powinien umożliwiać przywrócenie hasła głównego administratora w przypadku jego utraty.

1.36 W ramach systemu, komunikacja pomiędzy hostem źródłowym, a magazynem powinna odbywać się wyłącznie bezpośrednio pomiędzy agentem backupu, a magazynem. Komunikacja nie może przechodzić przez serwer backupu ani żaden inny komponent, którego awaria sparaliżowałaby działanie Systemu. System nie może posiadać pojedynczego punktu awarii.

1.37 System musi działać w zgodzie z regułą Zero-knowledge Encryption. Oznacza to, że wszelkie sekrety muszą być przechowywane w centralnym Managerze Haseł w postaci zaszyfrowanej algorytmem AES i być udostępniane agentowi dopiero w momencie rozpoczęcia wykonywania kopii zapasowej. Sekrety nie mogą być przechowywane w konfiguracji agenta na zabezpieczanym urządzeniu.

1.38 Aplikacje klienckie muszą wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn – żaden inny element Systemu, nie powinien brać udziału w przesyłaniu danych.

1.39 System musi wspierać instalację oraz uruchomienia agenta backupowego na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych min. o systemy:

- Debian: 9+,
- Ubuntu: 16.04+,
- Fedora: 29+,
- centOS: 7+,
- RHEL: 6+,
- openSUSE: 15+,
- SUSE Enterprise Linux (SLES): 12 SP2+,
- macOS: 10.13+,
- Windows: 7, 8.1, 10(1607+),
- Windows Server: 2008 R2+, • Hyper-V 2019+,
- VMware: 6.7+.

2 Środowiska fizyczne i bazy danych

2.1 System musi umożliwiać tworzenie grup urządzeń w celu automatyzacji procesów podczas pracy z urządzeniami.

2.2 System musi posiadać możliwość tworzenia zadań dla grupy urządzeń oraz dla wybranych urządzeń.

2.3 System musi pozwalać na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej.

2.4 System musi pozwalać na zabezpieczanie zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption.

2.5 System jest niezależny od wersji Microsoft SQL i musi umożliwiać przywracanie danych SQL dla tej samej lub nowszej wersji.

2.6 System musi obsługiwać również narzędzia RMAN firmy Oracle do tworzenia kopii zapasowych i odzyskiwania. Dodatkowo system musi obsługiwać funkcję przyrostowego scalania danych.

2.7 System musi wspierać odtwarzanie pojedynczych plików z systemów Windows oraz Linux.

2.8 W przypadku niedostępności źródła danych, system musi oczekiwać na powrót dostępności źródła danych przez określony przez administratora okres. W przypadku braku powrotu dostępności źródła, system musi podjąć ustaloną przez administratora liczbę prób kontynuacji kopii. W przypadku powrotu źródła danych system musi kontynuować zadanie backupu od momentu, w którym wystąpiła niedostępność źródła - system nie może rozpoczynać zadania od punktu początkowego i rozpoczynać przesyłania kopii od zera. W przypadku braku powrotu źródła danych system powinien zakończyć zadanie błędem.

2.9 System może odzyskiwać dane Bare Metal Restore na oryginalnym sprzęcie lub na różnych komputerach i serwerach z automatycznym dopasowaniem sterowników oraz możliwością dodania sterowników przez użytkownika.

2.10 System powinien umożliwiać uruchamianie procesu Bare Metal Restore z dowolnego bootowalnego nośnika danych.

2.11 System powinien wspierać odtwarzanie danych w scenariuszach P-2-P, P-2-V, V-2-P, V-2-V.

2.12 System umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie (RAW, VHD, VHDX, VMDK).

2.13 System musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL) oraz z prawami dostępu. Funkcjonalność ta musi być możliwa do skonfigurowania przez administratora na etapie konfiguracji procesu przywracania danych.

2.14 System musi umożliwiać przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows).

3 Środowiska wirtualne

3.1 System musi wspierać kopię w trybie application-aware dla wszystkich wspieranych wirtualizatorów.

3.2 System musi umożliwiać wykonywanie kopii maszyn wirtualnych z zastosowanie zaawansowanych metod transportu (HotAdd, SAN, LAN), w tym metodami LAN-Free, tj. takimi, które podczas wykonywania backupu nie obciążają interfejsów sieciowych maszyn wirtualnych.

3.3 System musi wykorzystywać mechanizmy Change Block Tracking oraz Replica Change Tracking dla wspieranych przez producenta platformach wirtualizacyjnych.

3.4 Rozwiązanie producenta musi być certyfikowane przez dostawcę platformy wirtualizacyjnej.

3.5 System musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage-u użytego do przechowywania kopii zapasowych.

3.6 Dla środowiska vSphere i Hyper-V rozwiązanie powinno umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).

3.7 System musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere.

3.8 System musi umożliwiać weryfikację odtwarzalności wirtualnych maszyn według własnego harmonogramu w dowolnym środowisku.

4 Aplikacje SaaS

4.1 System musi mieć możliwość zarządzania zadaniami z tej samej konsoli dla Microsoft 365 minimum na poziomie, skrzynek pocztowych, onedrive, kontaktów, kalendarza.

4.2 System musi umożliwiać przywracanie danych Microsoft 365: do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku .pst oraz do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji)

4.3 System musi umożliwiać granularne odtwarzanie danych, tj. pojedynczych plików z kopii obrazu dysku oraz pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365.

4.4 System musi umożliwiać zabezpieczanie środowisk Git, w tym GitHub, GitLab oraz Bitbucket wraz z metadanymi

4.5 System musi umożliwiać odtworzenie dowolnego środowiska Git w dowolnym innym środowisku Git, tzw. odtwarzanie crossowe.

4.6 System musi umożliwiać zabezpieczenie metadanych zebranych wokół repozytorium w ramach zabezpieczanego środowiska Git.

4.7 System musi umożliwiać odtwarzanie metadanych repozytorium Git do dowolnego innego środowiska Git w przypadku chęci odtworzenia repozytorium.

4.8 System musi umożliwiać zabezpieczenie środowisk Jira

4.9 System musi umożliwiać odtworzenie środowiska Jira do chmury lub środowiska lokalnego.

5 Minimalne parametry systemu

5.1 Obudowa RACK rozmiar: min: 1U,

5.2 Procesor: min. 8 rdzeni, min. 16 wątków. Minimalna częstotliwość bazowa procesora: 2.6GHz,

5.3 Pamięć RAM: Min. 16GB DDR4,

5.4 Wymagane min. 24TB liczona po wykonaniu konfiguracji dysków w RAID 5 przestrzeni dostępnej na przechowywanie danych.

5.5 Osobne dyski SSD M.2 nVME działające w redundancji RAID1 w celu instalacji warstwy oprogramowania i systemu operacyjnego,

5.6 Redundantne zasilanie,

5.7 Interfejsy sieciowe:

- Min. 2szt. 1GbE,
- Min. 2 x 10GbE

5.8 4x patchcord kat. 7 o długości 5 metrów.

6 Wsparcie techniczne (gwarancja), licencjonowanie

6.1 Wsparcie na rozwiązanie musi być obsługiwane w języku polskim.

6.2 Wsparcie techniczne musi być świadczone bezpośrednio producenta lub autoryzowany przez producenta serwis.

6.3 Możliwość zgłaszania problemów systemowych bezpośrednio z poziomu interfejsu zarządzania w formie czatu.

6.4 Producent wraz z systemem musi udostępnić materiały szkoleniowe w j. polskim (minimum dostęp do bazy wiedzy, materiałów wideo oraz kart produktów).

6.5 Wsparcie techniczne musi umożliwiać korzystanie z połączeń zdalnych, systemu do zgłaszania problemów z systemem oraz wsparcia telefonicznego.

6.6 W ramach wsparcia technicznego Zamawiający musi mieć dostęp do osoby po stronie Dostawcy dedykowanej do obsługi zgłoszeń technicznych, doraźnej pomocy i bieżącej pomocy w utrzymania infrastruktury Zamawiającego.

6.7 Dostawca musi dostarczyć bezpośredni numer telefonu oraz adres e-mail do dedykowanej dla klienta osoby.

6.8 Licencje w ramach rozwiązania musza obejmować zabezpieczenie: nielimitowanej ilości maszyn wirtualnych, nielimitowanej ilości serwerów fizycznych, nielimitowanej ilości stacji roboczych.

6.9 Licencje na system muszą być dostępne w opcji wieczystej.

6.10 Wsparcie techniczne producenta oraz gwarancja muszą zostać dostarczona na min. 12 miesięcy w trybie rozwiązania Następnego Dnia Roboczego

6.11 Licencje powinny umożliwiać replikacje kopii zapasowych na własne zasoby.

6.12 Licencje powinny umożliwiać korzystanie z przestrzeni chmurowej dostarczonej bezpośrednio przed producenta systemu, min. 4,5TB przez cały okres trwania wsparcia technicznego dostarczonej na oprogramowanie.

7 Zakres prac wdrożeniowych

7.1 Dostarczenie urządzenie do siedziby Zamawiającego

7.2 Fizyczna instalacja urządzeń w szafach RACK.

7.3 Podłączenie i konfiguracja urządzenia.

7.4 Wdrożenie musi zostać realizowane bezpośrednio przez producenta oferowanego systemu backupowego lub dostawcę posiadającego certyfikowanego inżyniera z ofertowanego systemu.

7.5 Wdrożenie musi zostać przeprowadzone przez producenta system.

7.6 Wdrożenie musi zakończyć się dostarczeniem dokumentacji powdrożeniowej, przygotowanej przez producenta systemu backupowego.

7.7 Wdrożenie powinno być zrealizowane tak, aby dostosować się do preferencji Zamawiającego.

7.8 Szkolenie z administracji systemem

- 7.8.1 Szkolenie może zostać przeprowadzone w formie zdalnej w języku polskim.
- 7.8.2 Szkolenie musi być realizowane przez producenta oferowanego systemu backupowego.
- 7.8.3 Szkolenie musi zostać przeprowadzone przez dedykowanego inżyniera producenta systemu.
- 7.8.4 Szkolenie musi zakończyć się imiennym certyfikatem dla administratorów uczestniczących w szkoleniu.
- 7.8.5 Szkolenie musi trwać minimum 8 godzin.

II. Urządzenie UTM

Zamawiający posiada urządzenie klasy UTM Stormshield SN310. W ramach projektu wymagane jest rozszerzenie, w celu stworzenia klastra urządzeń, co pozwoli na ograniczenie ryzyka związanego z awarią jednego urządzenia. Dlatego Zamawiający oczekuje dostarczenia drugiego urządzenia Stormshield SN310.

1 Wsparcie techniczne (gwarancja), licencjonowanie

1.1 Zamawiający wymaga dostarczenie licencji na antywirus, antyspam, filtrowanie stron internetowych, IPS (Intrusion Prevention System) i VPN do 30.06.2026 roku.

1.2 Gwarancja na urządzenie minimum 1 rok.

2 Równoważność

Zamawiający dopuszcza zaoferowanie urządzeń równoważnych, poprzez które należy rozumieć oferowane urządzenia o parametrach nie gorszych od posiadanego Stormshield SN310.

2.1 Procesor: A385 ARMv7 2.0GHz

2.2 Pamięć masowa: 32 GB SSD

2.3 Porty sieciowe: 8 portów 1Gbe Ethernet

2.4 Porty USB: 1 x USB 3.0, 1 x USB 2.0

2.5 Slot na kartę SD: Tak, obsługuje karty SDHC i SDXC do 2 TB
2.6 Wydajność zapory ogniowej: Do 3 Gbps
2.7 Wydajność VPN: Do 1 Gbps
2.8 Wydajność IPS: Do 1 Gbps
2.9 Zarządzanie: WebGUI, CLI (Command Line Interface)
2.10 Chłodzenie: Bez wentylatora (fanless)
2.11 Wymagane licencje: antywirus, antyspam, filtrowanie stron internetowych, IPS (Intrusion Prevention System) i VPN
2.12 Zamawiający wymaga dostarczenie licencji na antywirus, antyspam, filtrowanie stron internetowych, IPS (Intrusion Prevention System) i VPN do 30.06.2026 roku.
2.13 Gwarancja na urządzenie minimum 12 miesięcy.

3 Zakres wdrożenia

3.1 Montaż przedmiotu zamówienia w szafie RACK
3.2 Wykonanie podłączeń kablowych
3.3 Rekonfiguracja urządzeń w celu ustawienia klastra
3.4 Wykonanie kopii zapasowej urządzeń
3.5 Przeszkolenie Zamawiającego z administracji urządzeniami.

III. Wymagania Końcowe i Jakościowe Dotyczące Dostawy

1. Wymagane jest dostarczenie wszystkich niezbędnych kabli sygnałowych (zarówno miedzianych jak i światłowodowych) wymaganych do uruchomienia dostarczonego przedmiotu zamówienia i sieciowych w miejscu jej instalacji.
2. Cały oferowany przedmiot zamówienia musi być fabrycznie nowy, nieużywany i nieregenerowany (wyklucza się urządzenia refurbished). Cały przedmiot zamówienia musi być kompletny i wolny od wad fizycznych i prawnych.
3. Dostarczone urządzenia sprzętowe muszą posiadać rok produkcji nie wcześniejszy niż rok kalendarzowy 2025.
4. W dniu składania ofert oraz w dniu dostawy zaoferowane urządzenia i oprogramowanie nie mogą figurować w publicznie dostępnych informacjach producenta jako produkty, dla których ogłoszono zakończenie sprzedaży (End-of-Sale - EOS) lub zakończenie wsparcia (End-of-Life - EOL).
5. Wszystkie dostarczone produkty muszą pochodzić z legalnego i autoryzowanego kanału dystrybucyjnego producenta.