**Załącznik Nr 8 do SWZ**

**OPIS PRZEDMIOTU ZAMÓWIENIA
do postępowania pn.**

**„Cyberbezpieczny Samorząd – ETAP II”**

**w ramach programu „Fundusze Europejskie na Rozwój Cyfrowy (FERC),
numer naboru: FERC.02.02-CS.01-001/23**

**Wymagania ogólne dla urządzeń i oprogramowania**

1. Dostarczony sprzęt musi być fabrycznie nowy (rok produkcji 2024/2025), nieużywany, nieregenerowany, kompletny, dostarczony w opakowaniu oryginalnym (opakowanie musi być nienaruszone i posiadać zabezpieczenie zastosowane przez producenta). Nie dopuszcza się zastosowania urządzeń tzw. „refurbished”, rozwiązań odnawianych oraz eksponowanych na wystawach czy prezentacjach.
2. Sprzęt musi być wolny od wad fizycznych i prawnych, musi być sprawny technicznie oraz musi pochodzić z autoryzowanego kanału dystrybucyjnego. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanych rozwiązań, potwierdzające pochodzenie urządzeń z oficjalnego kanału dystrybucyjnego producenta.
3. Dostarczone oprogramowanie musi być nowe, nieużywane, nieaktywowane wcześniej na innym urządzeniu, dostarczone w najnowszej stabilnej wersji pochodzącej z oficjalnego kanału dystrybucyjnego producenta oprogramowania, nieobciążone prawami na rzecz osób trzecich. Dostarczone oprogramowanie i wszelkie jego nośniki (o ile występują) muszą być wolne od wad fizycznych i prawnych. Oprogramowanie musi być opatrzone we wszystkie atrybuty oryginalności i legalności wymagane przez producenta oprogramowania w zależności od dostarczanej wersji oprogramowania.
4. Serwis w ramach udzielonej gwarancji będzie realizowany bezpośrednio przez producenta i/lub we współpracy z autoryzowanym partnerem serwisowym producenta.
5. Wszystkie urządzenia powinny być zgodne z normami UE oraz powinny posiadać certyfikację oraz oznaczenie CE.
6. W formularzu ofertowym należy podać nazwę producenta, model, symbol (nazwę handlową) oraz parametry oferowanego rozwiązania (jeśli są wymagane) umożliwiające jednoznaczną weryfikację oferowanej konfiguracji oraz w celu identyfikacji należy podać pełną nazwę handlową oferowanego oprogramowania.

**Warunki dotyczące realizacji dostaw i odbiorów:**

1. Wykonawca na swój koszt i ryzyko dostarczy przedmiot zamówienia, zgodny z wymaganiami przedstawionymi w niniejszym dokumencie.
2. Wykonawca w cenie oferty uwzględni wszystkie koszty niezbędne do realizacji dostawy, w tym rozładunek, wniesienie oraz utrzymanie porządku w czasie rozładunku prowadzonego na terenie urzędu.
3. Wykonawca, co najmniej na 3 dni przed dniem planowanej dostawy sprzętu, dokona jej awizacji, to znaczy skontaktuje się z Zamawiającym w celu ustalenia miejsca i potwierdzenia konkretnego terminu dostawy.
4. Dostawa sprzętu odbędzie się w dniu roboczym, od poniedziałku do piątku, w godzinach 8:00 - 14:00, transportem zapewnionym przez Wykonawcę, na jego koszt i ryzyko wraz z wniesieniem do miejsca wskazanego przez Zamawiającego.
5. Do czasu odbioru sprzętu przez Zamawiającego, ryzyko wszelkich niebezpieczeństw związanych z jego ewentualnym uszkodzeniem lub utratą ponosi Wykonawca.
6. Wraz ze sprzętem Wykonawca zobowiązany jest przekazać Zamawiającemu listę numerów seryjnych dostarczonych urządzeń wszelką dokumentację dostarczoną przez producenta sprzętu.
7. W ramach procedury odbioru, Zamawiający zastrzega sobie w przypadku wątpliwości prawo do przeprowadzenia weryfikacji oryginalności i legalności dostarczonego przez Wykonawcę oprogramowania bezpośrednio u producenta oprogramowania, przed podpisaniem protokołu odbioru w sposób, który uzna za bezsporny. W przypadku wykrycia, że dostarczone oprogramowanie jest nieoryginalne (nielegalne), nie jest nowe, było już używane lub było już wcześniej aktywowane, Zamawiający w takiej sytuacji odmówi przyjęcia licencji oprogramowania i wezwie Wykonawcę do usunięcia nieprawidłowości w wyznaczonym terminie.

Szczegółowe wymagania w zakresie parametrów technicznych i funkcjonalnych poszczególnych elementów infrastruktury zostały określone w dalszej części dokumentu.

**CZĘŚĆ 1:**

**OBSZAR KOMPETENCYJNY**

1. **Zakup szkoleń specjalistycznych dla administratorów systemów informatycznych, obejmujących zarządzanie i konfiguracje infrastrukturą - Szkolenie Vmware vSphere: Instalacja, konfiguracja i zarządzanie.**

|  |  |
| --- | --- |
| **Kryterium** | **Wymagania minimalne dla organizowanego szkolenia** |
| Plan szkolenia | 1. Przegląd vSphere i wirtualizacji
* Wprowadzenie do koncepcji i znaczenia wirtualizacji.
* Szczegółowe omówienie vSphere i jego elementów.
1. Instalacja i konfiguracja ESXi
* Wprowadzenie do ESXi: Podstawy i znaczenie ESXi w środowisku VMware.
* Wymagania i instalacja: Przegląd wymagań i procesu instalacji ESXi.
* Konfiguracja hosta ESXi: Szczegółowe kroki konfiguracji hosta.
* Laboratoria i demonstracje: Praktyczne ćwiczenia z instalacji i konfiguracji.
1. Wdrażanie i konfiguracja vCenter
* Rola i znaczenie vCenter w zarządzaniu środowiskiem VMware.
* Przegląd komponentów i usług vCenter.
* Omówienie licencji i możliwości skalowania.
* Techniki i narzędzia do zarządzania zasobami.
* Zarządzanie dostępem i uprawnieniami użytkowników.
1. Konfiguracja sieci vSphere
* Wprowadzenie do sieci wirtualnych i ich typów.
* Standardowe i rozproszone przełączniki
* Ćwiczenia z konfiguracji i zarządzania siecią w środowisku vSphere.
1. Konfiguracja przechowywania danych w vSphere
* Wprowadzenie do koncepcji i typów przechowywania danych.
* VMFS i NFS Datastores - konfiguracja i zarządzanie magazynami danych.
* Fibre Channel i iSCSI Storage - konfiguracja różnych typów przechowywania.
* Laboratoria i ćwiczenia praktyczne: Praktyczne zastosowanie wiedzy o przechowywaniu danych.
1. Wdrażanie maszyn wirtualnych
* Proces tworzenia i konfiguracji maszyn wirtualnych.
* Wykorzystanie szablonów i zarządzanie bibliotekami.
* Instalacja i aktualizacja narzędzi VMware, zarządzanie sprzętem wirtualnym.
* Laboratoria i symulacje: Praktyczne ćwiczenia z tworzenia i zarządzania VM.
1. Zarządzanie Maszynami Wirtualnymi
* Migracja Maszyn Wirtualnych: Omówienie różnych typów migracji, w tym vSphere vMotion.
* Zarządzanie Snapshots: Techniki zarządzania snapshotami
1. Wdrażanie i Konfiguracja Klastrów vSphere
* Przegląd Klastrów vSphere: Podstawy tworzenia i zarządzania klastrami vSphere.
* vSphere Distributed Resource Scheduler (DRS): Konfiguracja i zarządzanie DRS w klastrach.
* vSphere High Availability (HA): Wprowadzenie do HA i scenariusze awarii.
* Architektura vSphere HA: Szczegółowe omówienie architektury i komunikacji w HA.
* Konfiguracja vSphere HA: Praktyczne wskazówki dotyczące konfiguracji i zarządzania HA.
 |
| Typ szkolenia | Szkolenie on-line, czas trwania minimum 2 dni |
| Certyfikat | Wymagany certyfikat, zaświadczenie ukończenia szkolenia lub potwierdzenie odbycia szkolenia - dokument wydany przez jednostkę prowadzącą szkolenie. |
| Pozostałe wymagania | Obowiązkiem Wykonawcy jest organizacja i przeprowadzenie szkolenia lub zakup szkolenia w zewnętrznej jednostce szkoleniowej.Zamawiający dopuszcza przekazanie Vouchera szkoleniowego (pisemnego zaświadczenia o uzyskaniu prawa do zamówienia szkolenia we wskazanej przez Wykonawcę placówce szkoleniowej), z możliwością wybrania przez Zamawiającego terminu szkolenia. |

1. **Zakup szkoleń specjalistycznych dla administratorów systemów informatycznych, obejmujących zarządzanie i konfiguracje infrastrukturą - Szkolenie Certified Stormshield Network Administrator (CSNA)**

|  |  |
| --- | --- |
| **Kryterium** | **Wymagania minimalne dla organizowanego szkolenia** |
| Plan szkolenia | 1. Rozpoczęcie pracy z urządzeniem:
* Rozpoczęcie pracy z urządzeniem i wprowadzenie do interfejsu administracyjnego.
* Ustawienia systemowe i uprawnienia administratorów.
* Instalacja licencji i aktualizacja systemu.
* Tworzenie kopii zapasowej i przywracanie konfiguracji
1. Zbieranie logów i monitorowanie:
* Przedstawienie kategorii zbieranych logów
* Wykresy historyczne i monitorowanie
1. Obiekty
* Typy obiektów oraz ich wykorzystanie
* Obiekty sieciowe i obiekt typu „router”
1. Konfiguracja sieci
* Tryby pracy urządzenia
* Typy interfejsów (Ethernet, modem, bridge, VLAN, GRETAP)
* Typy routingu oraz ich priorytety
1. Translacja adresów sieciowych (NAT)
2. Translacja połączeń wychodzących (maskarada)
3. Translacja połączeń przychodzących (przekierowanie)
4. Translacja dwukierunkowa (jeden do jeden)
5. Filtrowanie ruchu sieciowego (Firewall)
6. Ogólne informacje dot. filtrowania ruchu i koncepcji śledzenia połączeń (Stateful inspection)
* Szczegółowy opis parametrów reguły Firewall
* Kolejność przetwarzania reguł Firewall i NAT
1. Ochrona aplikacji
* Implementacja filtrowania URL dla ruchu http i https
* Konfigurowanie skanowania antywirusowego i modułu Breach Fighter
* Moduł IPS i stosowanie profili inspekcji
1. Użytkownicy i uwierzytelnianie
2. Konfiguracja usługi katalogowej
* Wprowadzenie do różnych metod uwierzytelniania (LDAP, Kerberos, Radius, certyfikat SSL, SPNEGO, SSO)
* Rejestracja użytkowników
* Uwierzytelnianie użytkowników za pomocą portalu uwierzytelniania
1. Wirtualne sieci prywatne (VPN)
* Koncepcje i ogólne informacje dotyczące protokołu IPSec VPN (IKEv1 i IKEv2)
* Tunele Site-to-Site z wykorzystaniem klucza współdzielonego (PSK)
* Tunele VTI
1. SSL VPN
* Zasada działania
* Konfiguracja
 |
| Typ szkolenia | Szkolenie on-line, czas trwania minimum 3 dni |
| Certyfikat | Wymagany certyfikat, zaświadczenie ukończenia szkolenia lub potwierdzenie odbycia szkolenia - dokument wydany przez jednostkę prowadzącą szkolenie. |
| Pozostałe wymagania | Obowiązkiem Wykonawcy jest organizacja i przeprowadzenie szkolenia lub zakup szkolenia w zewnętrznej jednostce szkoleniowej.Zamawiający dopuszcza przekazanie Vouchera szkoleniowego (pisemnego zaświadczenia o uzyskaniu prawa do zamówienia szkolenia we wskazanej przez Wykonawcę placówce szkoleniowej), z możliwością wybrania przez Zamawiającego terminu szkolenia. |

1. **Zakup szkoleń specjalistycznych dla administratorów systemów informatycznych, obejmujących zarządzanie i konfiguracje infrastrukturą - Szkolenie Certified Stormshield Network Expert (CSNE)**

|  |  |
| --- | --- |
| **Kryterium** | **Wymagania minimalne dla organizowanego szkolenia** |
| Plan szkolenia | 1. Szczegółowe omówienie działania modułu IPS od Stormshield:
* Różnice pomiędzy IPS a IDS.
* moduł IPS.
* Różne tryby analizy.
* Profile oparte na protokołach i aplikacjach.
1. Infrastruktura klucza publicznego:
* Podstawy szyfrowania symetrycznego i asymetrycznego.
* Typy szyfrowania.
* Infrastruktura klucza publicznego w rozwiązaniach Stormshield.
* Tworzenie urzędu certyfikacji, certyfikatów serwera i użytkowników.
1. SSL Proxy:
* Zasada działania.
* Konfiguracja SSL Proxy.
* Zaawansowana konfiguracja tuneli IPSec VPN.
* Szczegółowy opis działania mechanizmu NAT traversal.
* Obsługa funkcji DPD (Dead Peer Detection).
* Architektura sieci VPN typu „gwiazda” i „mesh”.
* NAT w sieciach IPSec VPN.
* Konfiguracja zapasowego - tunelu IPSec VPN.
* Konfiguracja tuneli Site-to-Site w oparciu - certyfikaty.
* Konfiguracja tuneli dla użytkowników mobilnych (Client-2-Site).
1. GRE i GRETAP:
* Zasada działania.
* Konfiguracja i instalacja.
1. Transparentne uwierzytelnianie użytkowników:
* Zasada działania.
* Metoda uwierzytelniania SPNEGO.
* Metoda uwierzytelniania oparta na certyfikatach SSL.
1. Wysoka dostępność (HA):
* Zasada działania.
* Kreator umożliwiający tworzenie i konfigurowanie klastra HA.
* Konfiguracja interfejsu sieciowego.
* Zaawansowana konfiguracja.
 |
| Typ szkolenia | Szkolenie on-line, czas trwania minimum 3 dni |
| Certyfikat | Wymagany certyfikat, zaświadczenie ukończenia szkolenia lub potwierdzenie odbycia szkolenia - dokument wydany przez jednostkę prowadzącą szkolenie. |
| Pozostałe wymagania | Obowiązkiem Wykonawcy jest organizacja i przeprowadzenie szkolenia lub zakup szkolenia w zewnętrznej jednostce szkoleniowej.Zamawiający dopuszcza przekazanie Vouchera szkoleniowego (pisemnego zaświadczenia o uzyskaniu prawa do zamówienia szkolenia we wskazanej przez Wykonawcę placówce szkoleniowej), z możliwością wybrania przez Zamawiającego terminu szkolenia. |

1. **Zakup szkoleń specjalistycznych dla administratorów systemów informatycznych, obejmujących zarządzanie i konfiguracje infrastrukturą - Szkolenie Safetica Administrator**

|  |  |
| --- | --- |
| **Kryterium** | **Wymagania minimalne dla organizowanego szkolenia** |
| Zakres szkolenia | 1. Wdrożenie rozwiązania
* Omówienie instalatora
* Wdrożenie serwera
* Wdrożenie klienta
1. Konsola Maintanance
* Kategoryzacja aplikacji oraz stron internetowych
* Zarządzanie bazą danych
* Ustawienia klienta
* Dezaktywacja modułów klienta
* Ustawienia integracji
1. Moduł Discovery
* Uruchomienie modułu Discovery
* Analiza potencjalnych wycieków danych
* Dostosowanie konsoli do własnych potrzeb, filtrowanie danych
1. Podstawowe DLP
* Szyfrowanie dysków Bitlockerem
* Strefy - konfiguracja dostępów dla urządzeń i portów
1. Zaawansowane DLP
* Reguły DLP - tryby polityk
* Reguły ogólne
* Reguły aplikacji
* Inteligentne wykrywanie danych osobowych
* Dzienniki DLP
 |
| Typ szkolenia | Szkolenie on-line, czas trwania minimum 2 dni |
| Certyfikat | Wymagany certyfikat, zaświadczenie ukończenia szkolenia lub potwierdzenie odbycia szkolenia - dokument wydany przez jednostkę prowadzącą szkolenie. |
| Pozostałe wymagania | Obowiązkiem Wykonawcy jest organizacja i przeprowadzenie szkolenia lub zakup szkolenia w zewnętrznej jednostce szkoleniowej.Zamawiający dopuszcza przekazanie Vouchera szkoleniowego (pisemnego zaświadczenia o uzyskaniu prawa do zamówienia szkolenia we wskazanej przez Wykonawcę placówce szkoleniowej), z możliwością wybrania przez Zamawiającego terminu szkolenia. |

1. **Zakup szkoleń specjalistycznych dla administratorów systemów informatycznych, obejmujących zarządzanie i konfiguracje infrastrukturą - Szkolenie Synology DSM Architect**

|  |  |
| --- | --- |
| **Kryterium** | **Wymagania minimalne dla organizowanego szkolenia** |
| Zakres szkolenia | 1. Zarządzanie przechowywaniem:
* Przestrzeń dyskowa - planowanie i konfiguracja.
* Pamięć podręczna SSD.
* Pamięć RAM - ustalanie potrzebnej ilości.
* System plików - Btrfs vs. ext4.
* Zabezpieczenie integralności danych.
1. Optymalizacja ustawień:
* Obsługa systemów UPS, Synology jako serwer UPS.
* Konfiguracja interfejsów sieciowych i kontroli przepływu danych.
* Agregacja portów sieciowych dla lepszej wydajności lub niezawodności.
* Powiadomienia & logi.
1. Usługi plików i foldery współdzielone:
* Ustawienia klasycznych protokołów dla płynnej komunikacji.
* Zarządzanie rozszerzonymi uprawnieniami ACL.
* Foldery współdzielone - funkcjonalność, zarządzanie & limity (Quota).
* WriteOnce / WORM.
* Szyfrowanie folderów współdzielonych - wprowadzenie do rozwiązania szyfrowania folderów współdzielonych.
* Szyfrowanie wolumenów - wprowadzenie do rozwiązania szyfrowania wolumenów.
* Menedżer kluczy - rozwiązanie do inteligentnego przechowywania kluczy szyfrowanych folderów współdzielonych.
* Szybkie klonowanie plików.
1. Snapshot Replication:
* Migawki - rozwiązanie w oparciu o system plików Btrfs.
* Migawki niezmienne (w oparciu o technologię WORM).
* Konfiguracja & wykonywanie migawek lokalnych.
* Metody odzyskiwania danych z migawek lokalnych.
* Migawki folderów szyfrowanych - wykonywanie & odzyskiwanie danych.
1. Funkcje bezpieczeństwa
* Blokowanie zakresów adresów IP.
* Ustawienia zapory i oprogramowania antywirusowego.
* Certyfikaty, wytyczne dotyczące haseł.
* Bezpieczne logowanie & uwierzytelnianie dwuelementowe (Secure SignIn, Windows Hello / Apple Touch ID / FIDO 2 jako klucze sprzętowe itd.).
* Security Advisor - dedykowane narzędzie diagnostyczne.
* Dobre praktyki jako środki zabezpieczające.
1. Konserwacja i migracja danych:
* Rozbudowa & migracja RAID.
* Metody migracji danych (sprzętowa & programowa).
* Migration Assistant.
* Rozwiązywanie problemów.
1. Pozostałe funkcje:
* Synology Directory Server jako kontroler domeny AD.
* Synology CMS jako system centralnego zarządzania urządzeniami NAS Synology.
* Synology Hybrid Share - hybrydowa przestrzeń dyskowa.
* Synology Active Insight - inteligentny monitorowanie stanu systemu DSM & aplikacji.
 |
| Typ szkolenia | Szkolenie on-line, czas trwania minimum 2 dni |
| Certyfikat | Wymagany certyfikat, zaświadczenie ukończenia szkolenia lub potwierdzenie odbycia szkolenia - dokument wydany przez jednostkę prowadzącą szkolenie. |
| Pozostałe wymagania | Obowiązkiem Wykonawcy jest organizacja i przeprowadzenie szkolenia lub zakup szkolenia w zewnętrznej jednostce szkoleniowej.Zamawiający dopuszcza przekazanie Vouchera szkoleniowego (pisemnego zaświadczenia o uzyskaniu prawa do zamówienia szkolenia we wskazanej przez Wykonawcę placówce szkoleniowej), z możliwością wybrania przez Zamawiającego terminu szkolenia. |

1. **Zakup szkoleń specjalistycznych dla administratorów systemów informatycznych, obejmujących zarządzanie i konfiguracje infrastrukturą - Szkolenie Synology Backup Architect**

|  |  |
| --- | --- |
| **Kryterium** | **Wymagania minimalne dla organizowanego szkolenia** |
| Zakres szkolenia | 1. Podstawowe informacje nt. kopii zapasowych:
* RPO & RTO.
* Porównanie metod tworzenia kopii zapasowych.
* Deduplikacja - charakterystyka i warianty wykorzystywane w Synology DSM.
* Zagrożenia & ryzyka utraty danych - przeciwdziałanie.
* Strategia kopii zapasowych.
1. Snapshot Replication:
* Migawki - opis rozwiązania w oparciu o system plików Btrfs.
* Konfiguracja & wykonywanie migawek lokalnych.
* Konfiguracja & wykonywanie replikacji migawek.
* Metody odzyskiwania danych z lokalnych & zreplikowanych migawek.
* Przełączanie i praca awaryjna w Snapshot Replication (charakterystyka, cele, różnice).
* Omówienie zagadnienia zajętości migawek.
1. Hyper Backup:
* Podstawowe informacji nt. zasad wykonywania kopii zapasowych przez Hyper Backup.
* Warianty tworzenia kopii zapasowych (rodzaje i miejsca docelowe).
* Kompleksowe omówienie wszystkich niezbędnych funkcjonalności (wersjonowanie, przechowywanie itd.).
* Kopia zapasowa szyfrowanych folderów współdzielonych.
* Ponowne przypisywanie zadań.
* Hyper Backup Vault jako kompleksowe narzędzie do zarządzania kopiami w kontenerach.
1. Kopie zapasowe na nośnik USB:
* Kopia zapasowa za pomocą Hyper Backup.
* Kopia zapasowa za pomocą USB Copy (opis wariantów kopii, wyzwalacze itd.).
* Porównanie obu metod.
1. Synology C2 Storage:
* Omówienie najważniejszych funkcji.
* Prezentacja działania usługi w praktyce.
1. Active Backup:
* Wprowadzenie do rozwiązania kopii zapasowej urządzeń końcowych.
* Omówienie najważniejszych cech pakietu (deduplikacja, kompresja, rotacja wersji, masowe wdrażanie agentów itd.).
* Zabezpieczenie PC & serwerów fizycznych (Windows & MacOS & Linux).
* Zabezpieczenie maszyn wirtualnych (HyperV i VMware) przy wykorzystaniu technologii CBT oraz RCT.
* Plikowa kopia zapasowa (SMB & Rsync).
* Omówienie podstawowych opcji przywracania (portal przywracania, odzyskiwanie bare-metal).
* Omówienie zaawansowanych metod przywracania danych (odzyskiwanie natychmiastowe bądź pełne w trybie Physical-to-Virtual lub do Virtual Machine Manager).
1. Active Backup for Microsoft 365 / Google Workspace
* Podstawy lokalnych kopii zapasowych Saas - prekonfiguracja usług.
* Kopie zapasowe danych, maili, kontaktów, kalendarzy, dysków.
* Przywracanie pojedynczych elementów i całych kont.
* Zarządzanie zadaniami tworzenia kopii zapasowych.
 |
| Typ szkolenia | Szkolenie on-line, czas trwania minimum 2 dni |
| Certyfikat | Wymagany certyfikat, zaświadczenie ukończenia szkolenia lub potwierdzenie odbycia szkolenia - dokument wydany przez jednostkę prowadzącą szkolenie. |
| Pozostałe wymagania | Obowiązkiem Wykonawcy jest organizacja i przeprowadzenie szkolenia lub zakup szkolenia w zewnętrznej jednostce szkoleniowej.Zamawiający dopuszcza przekazanie Vouchera szkoleniowego (pisemnego zaświadczenia o uzyskaniu prawa do zamówienia szkolenia we wskazanej przez Wykonawcę placówce szkoleniowej), z możliwością wybrania przez Zamawiającego terminu szkolenia. |

1. **Zakup szkoleń specjalistycznych dla administratorów systemów informatycznych, obejmujących zarządzanie i konfiguracje infrastrukturą - Szkolenie Synology Collaboration Architect**

|  |  |
| --- | --- |
| **Kryterium** | **Wymagania minimalne dla organizowanego szkolenia** |
| Zakres szkolenia | 1. Synology Drive:
* Podstawy & opis technologii - SPR, Delta Sync, Intelliversioning, synchronizacja na żądanie.
* Tryby synchronizacji i folder domowy.
* Porównanie metod udostępniania plików dla użytkowników - udostępnianie wewnętrzne vs. udostępnianie publiczne.
* Foldery zespołów i Konsola Administratora.
* Synology Drive ShareSync.
1. Synology Office:
* Instalacja i zawarte aplikacje.
* Wersjonowanie.
* Dokumenty szyfrowane.
* Uprawnienia dostępu do plików/folderów.
* Import/export dokumentów.
* Praca na plikach „w czasie rzeczywistym”.
1. Synology Chat:
* Obsługa konta.
* Kanał vs. konwersacja (publiczny vs. prywatny).
* Szyfrowanie korespondencji.
1. Synology Calendar & Contact:
* Synchronizacja danych pomiędzy różnymi platformami.
* Synology Contact - import kontaktów z platformy Microsoft 365.
* Natywna integracja z innymi pakietami Synology z działu produktywności (MailPlus Client, Chat, Drive itd.).
* Zarządzanie kontaktami & kalendarzami.
1. Synology Note Station
* Podstawowe funkcje oraz zastosowania (tworzenie notesów, archiwów itd.).
* Wykorzystanie wtyczki Web Clipper to przechwytywania zawartości maili oraz stron internetowych.
 |
| Typ szkolenia | Szkolenie on-line, czas trwania minimum 2 dni |
| Certyfikat | Wymagany certyfikat, zaświadczenie ukończenia szkolenia lub potwierdzenie odbycia szkolenia - dokument wydany przez jednostkę prowadzącą szkolenie. |
| Pozostałe wymagania | Obowiązkiem Wykonawcy jest organizacja i przeprowadzenie szkolenia lub zakup szkolenia w zewnętrznej jednostce szkoleniowej.Zamawiający dopuszcza przekazanie Vouchera szkoleniowego (pisemnego zaświadczenia o uzyskaniu prawa do zamówienia szkolenia we wskazanej przez Wykonawcę placówce szkoleniowej), z możliwością wybrania przez Zamawiającego terminu szkolenia. |

1. **Zakup szkoleń dla kadry pracowniczej z cyberbezpieczeństwa.**

|  |  |
| --- | --- |
| **Kryterium** | **Wymagania minimalne dla organizowanego szkolenia** |
| Zakres szkolenia | * + - 1. Główne założenia i wymagania prawne RODO, KRI, KSC.
			2. Incydent bezpieczeństwa komputerowego i RODO - zasady postepowania w przypadku jego wystąpienia.
			3. Naruszenie ochrony danych osobowych i zasady postepowania w przypadku jego wystąpienia.
			4. Podstawowe zasady bezpieczeństwa (bezpieczeństwo fizyczne):
	+ Zasada czystego biurka;
	+ Zasada czystego ekranu;
	+ Zasada czystego wydruku;
	+ Zasada czystego kosza;
		- 1. Polityka bezpiecznych haseł (menadżer haseł, generowanie i dobór haseł, postępowanie z hasłami).
			2. Najczęściej wykorzystywane metody ataków (socjotechnika, phishing, spoofing, sim swap, ataki przez strony www, telefon, spam).
			3. Podstawowe metody obrony i weryfikacji prób ataków.
			4. Omówienie ataków na przykładach.
			5. Rozmowa otwarta - podsumowanie szkolenia
 |
| Typ szkolenia | Szkolenie stacjonarne realizowane w formie wykładu, w podziale na grupy, realizowane w siedzibie Urzędu Gminy w Jaśle.Zamawiający przewiduje minimum 2 godziny lekcyjne dla każdej grupy przy założeniu, że jedna godzina lekcyjna trwa 45 minut. |
| Certyfikat | Wymagany certyfikat, zaświadczenie ukończenia szkolenia lub potwierdzenie odbycia szkolenia - dokument wydany przez jednostkę prowadzącą szkolenie. |
| Obowiązki Wykonawcy | Obowiązkiem Wykonawcy będzie zapewnienie:1. Pakietu materiałów szkoleniowych.
2. Wydanie uczestnikom szkolenia zaświadczeń o ukończeniu szkolenia.
3. Prowadzenie dokumentacji w formie listy obecności uczestników szkolenia.
4. Sprzętu elektronicznego (laptop, projektor) niezbędnego do prowadzenia szkolenia.
 |
| Obowiązki Zamawiającego | Obowiązkiem Zamawiającego będzie zapewnienie:* + - 1. Nieodpłatne udostępnienie lokalu (szali szkoleniowej dla wymaganej liczby uczestników) z dostępem do Internetu oraz energii elektrycznej.
			2. Rekrutacji osób biorących udział w szkoleniach oraz ustalenie składu grup.
 |
| Pozostałe wymagania | Obowiązkiem Wykonawcy jest organizacja i przeprowadzenie szkolenia lub zakup szkolenia w zewnętrznej jednostce szkoleniowej.Zamawiający dopuszcza przekazanie Vouchera szkoleniowego (pisemnego zaświadczenia o uzyskaniu prawa do zamówienia szkolenia we wskazanej przez Wykonawcę placówce szkoleniowej), z możliwością wybrania przez Zamawiającego terminu szkolenia. |

**CZĘŚĆ 2:**

**OBSZAR TECHNICZNY**

1. **Zakup dysków twardych do NAS**

|  |  |
| --- | --- |
| **Kryterium** | **Wymagane minimalne parametry lub funkcjonalności** |
| Typ | W ofercie wymagane jest podanie producenta, modelu/symbolu/nazwy handlowej, pojemności oraz okresu gwarancji |
| Ilość | 2 sztuki o pojemności min. 10TB każdy8 sztuk o pojemności min. 16TB każdy |
| Zastosowanie | Dysk twardy do serwera NAS Synology RS1221RP+ |
| Wymagania techniczne | Dyski twarde klasy Enterprise przystosowane do zapisu ciągłego, kompatybilne z urządzeniem NAS Synology RS1221RP+. |
| Gwarancja i serwis | Min. 3 lata (36 miesięcy) |

1. **Zakup dysków zewnętrznych USB w celu przechowywania odseparowanych od sieci kopii zapasowych**

|  |  |
| --- | --- |
| **Kryterium** | **Wymagane minimalne parametry lub funkcjonalności** |
| Typ | W ofercie wymagane jest podanie producenta, modelu/symbolu/nazwy handlowej, pojemności oraz okresu gwarancji |
| Ilość | 2 zestawy |
| Wymagania techniczne | Pojemność 10TB, interfejs w standardzie USB 3.0 lub nowszy.Bezpieczeństwo: 256-bitowe szyfrowanie danych AES. |
| Gwarancja i serwis | Min. 2 lata (24 miesiące) |

1. **Zakup dysków do macierzy produkcyjnej - typ 1**

|  |  |
| --- | --- |
| **Kryterium** | **Wymagane minimalne parametry lub funkcjonalności** |
| Typ | W ofercie wymagane jest podanie producenta, modelu/symbolu/nazwy handlowej, pojemności oraz okresu gwarancji |
| Ilość | 7 sztuk |
| Zastosowanie | Dysk twardy do macierzy Dell EMC ME5024 |
| Wymagania techniczne | W celu zachowania pełnej kompatybilności z posiadanymi dyskami w macierzy Zamawiający wymaga dostarczenia dysków talerzowych HDD 2,5 cala o pojemności 2.4TB, interfejs SAS 12Gb/s, w pakiecie obudowa dysku do instalacji Hot-Plug. |
| Gwarancja i serwis | Dostarczone dyski muszą przejąć warunki gwarancyjne macierzy, w której będą zainstalowane i muszą być objęte gwarancją producenta macierzy. |

1. **Zakup dysków do macierzy produkcyjnej - typ 2**

|  |  |
| --- | --- |
| **Kryterium** | **Wymagane minimalne parametry lub funkcjonalności** |
| Typ | W ofercie wymagane jest podanie producenta, modelu/symbolu/nazwy handlowej, pojemności oraz okresu gwarancji |
| Ilość | 5 sztuk |
| Zastosowanie | Dysk twardy do macierzy Dell EMC ME5024 |
| Wymagania techniczne | W celu zachowania pełnej kompatybilności z posiadanymi dyskami w macierzy Zamawiający wymaga dostarczenia dysków SSD 2,5 cala o pojemności 1.92TB, interfejs SAS 24Gb/s, w pakiecie obudowa dysku do instalacji Hot-Plug. |
| Gwarancja i serwis | Dostarczone dyski muszą przejąć warunki gwarancyjne macierzy, w której będą zainstalowane i muszą być objęte gwarancją producenta macierzy. |

1. **Zakup urządzenia klasy UTM z subskrypcjami i wsparciem technicznym w okresie trwania projektu - typ 2**

|  |  |
| --- | --- |
| **Kryterium** | **Wymagane minimalne parametry lub funkcjonalności** |
| Typ | W ofercie wymagane jest podanie producenta, modelu/symbolu/nazwy handlowej, nazw serwisów i licencji oraz okresu gwarancji |
| Ilość | 1 zestaw |
| Wymagania techniczne i funkcjonalne | Wymagane jest dostarczenie dodatkowego (zapasowego) urządzenia pełniącego funkcję standby w klastrze wysokiej dostępności z urządzeniem podstawowym (master) będącym w posiadaniu Zamawiającego, tj. FortiGate-60F.Urządzenie typu slave musi mieć identyczne parametry wydajnościowe oraz sprzętowe jak podstawowa jednostka master. |
| Serwisy i licencje | Wraz z urządzeniem wymagane jest dostarczenie licencji i serwisów pozwalających korzystać z funkcjonalności klastra HA przy założeniu, ze urządzenie master posiada licencję Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, Web & Video Filtering, Antispam Service, and 24x7 FortiCare)Licencje oraz serwisy powinny mieć zapewnione aktualizację oraz wsparcie techniczne w okresie realizacji projektu do 30.06.2026 r. |
| Gwarancja i serwis | Min. 2 lata (24 miesiące) |

1. **Zakup urządzenia klasy UTM z subskrypcjami i wsparciem technicznym w okresie trwania projektu - typ 3**

|  |  |
| --- | --- |
| **Kryterium** | **Wymagane minimalne parametry lub funkcjonalności** |
| Typ | W ofercie wymagane jest podanie producenta, modelu/symbolu/nazwy handlowej, nazw serwisów i licencji oraz okresu gwarancji |
| Ilość | 1 zestaw |
| Wymagania techniczne i funkcjonalne | Wymagane jest dostarczenie dodatkowego (zapasowego) urządzenia pełniącego funkcję standby w klastrze wysokiej dostępności z urządzeniem podstawowym (master) będącym w posiadaniu Zamawiającego, tj. Stormshield SN310.Urządzenie typu slave musi mieć identyczne parametry wydajnościowe oraz sprzętowe jak podstawowa jednostka master. |
| Serwisy i licencje | Wraz z urządzeniem wymagane jest dostarczenie licencji i serwisów pozwalających korzystać z funkcjonalności klastra HA przy założeniu, ze urządzenie master posiada licencję UTM Security Pack (Essentials Security Pack) + Next Business DayLicencje oraz serwisy powinny mieć zapewnione aktualizację oraz wsparcie techniczne w okresie realizacji projektu do 30.06.2026 r. |
| Gwarancja i serwis | Min. 2 lata (24 miesiące) |

1. **Zakup utrzymanie wsparcia technicznego wraz z subskrypcjami dla posiadanego UTM w okresie trwania projektu - typ 2**

|  |  |
| --- | --- |
| **Kryterium** | **Wymagane minimalne parametry lub funkcjonalności** |
| Typ | W ofercie wymagane jest podanie nazwa serwisów i/lub licencji oraz okresu wsparcia |
| Ilość | 1 zestaw |
| Rodzaj wsparcia z subskrypcjami | Zamawiający wymaga dostarczenia pakietów licencji dotyczących wsparcia technicznego dla funkcji bezpieczeństwa powiązanych z posiadanym urządzeniem Stormshield SN 310, tj.:- Essentials Security Pack- Next Business Day (wymiana urządzenia)Licencje oraz serwisy powinny mieć zapewnione aktualizację oraz wsparcie techniczne w okresie realizacji projektu do 30.06.2026 r. |

1. **Zakup utrzymania wsparcia technicznego wraz z subskrypcjami ze wsparciem w okresie trwania projektu dla posiadanego oprogramowania do realizacji kopii zapasowych.**

|  |  |
| --- | --- |
| **Kryterium** | **Wymagane minimalne parametry lub funkcjonalności** |
| Typ | W ofercie wymagane jest podanie nazwa serwisów i/lub licencji oraz okresu wsparcia |
| Ilość | 1 zestaw zawierający wsparcie techniczne dla 3 licencji obejmujących łączne 15 instancji. |
| Rodzaj wsparcia z subskrypcjami | Zamawiający wymaga dostarczenia pakietu aktualizacji wsparcia technicznego dla posiadanych licencji stosowanej do realizacji kopii zapasowych pod nazwą „Veeam Backup Essentials Universal Perpetual License. Includes Enterprise Plus Edition features.” |
| Okres ochrony | Licencje oraz serwisy powinny mieć zapewnione aktualizację oraz wsparcie techniczne w okresie realizacji projektu do 30.06.2026 r. |

1. **Zakup zarządzalnych przełączników sieciowych - typ 1.**

|  |  |
| --- | --- |
| **Kryterium** | **Wymagane minimalne parametry lub funkcjonalności** |
| Typ | W ofercie wymagane jest podanie producenta, modelu/symbolu/nazwy handlowej, okresu gwarancji oraz wyposażenia. |
| Ilość | 3 zestawy |
| Wymagania techniczne i funkcjonalne | Porty przełącznika: minimum 48x 10/100/1000Base-T RJ45 wpierające PoE/PoE+ oraz minimum 4 porty 10GE SFP+; Porty SFP+ 10GE obsługujące moduły 1GE SFP;Stackowanie: możliwość połączenia minimum 4 przełączników w stos za pomocą portów SFP+ bez dedykowanego okablowaniaPort konsolowy: RJ45 (RS-232)Port zarządzania: RJ45 (10/100Base-T RJ45)Port USB: minimum 1 port co najmniej w standardzie 2.0Szybkość przełączania: minimum 176 Gb/s Przepustowość: minimum 131 Mp/s (dla pakietów 64Kb) Bufor pakietów: minimum 3MB Ramki Jumbo: minimum 10kTablica adresów MAC: minimum 16k Adresy MAC - Multicast: minimum 4kTablica ACL: minimum 512Tablica VLAN: minimum 4kTablica routingu: minimum 512 dla IPv4, w tym IPv6. Dopuszcza się rozwiązania współdzielące tablicę routingu dla IPv4 oraz IPv6 w maksymalnej proporcji 4:1.Tablica ARP: minimum 512Pamięć Flash: minimum 32MB + 128MB NANDPamięć RAM: minimum 256MBObsługa PoE: minimum IEEE 802.3 af/atBudżet mocy PoE: minimum 740WTemperatura pracy: zakres minimum 0°C - 50°CWilgotność względna: zakres minimum 10% - 90% (bez kondensacji)Zasilanie: zabudowany zasilacz - 230V ACRedundantne zasilanie: zabudowany zasilacz - 48V DCPobór mocy: maksymalnie 897WZabezpieczenie przeciwprzepięciowe: minimum 4kVAlgorytm pracy: Store and ForwardObsługa VLAN: Voice VLAN, Port based VLAN, MAC based VLAN, Protocol based VLAN, Private VLAN, GVRP, IEEE 802.1Q, Normal QinQ, Flexible QinQDHCP: IPv4/IPv6 DHCP Client,IPv4/IPv6 DHCP Relay, Option 82, IPv4/IPv6 DHCP Snooping,IPv4/IPv6 DHCP ServerProtokoły drzewa rozpinającego: IEEE802.1D (STP), IEEE802.1W (RSTP), IEEE802.1S (MSTP), Multi-Process MSTP, Root Guard, BPDU guard, BPDU forwarding, Protekcja ringowa: ITU-T G.8032 - recovery time < 50ms, Loopback Detection, Fast LinkProtokoły routingu: Static Routing, RIPv1/v2, RIPng, OSPFv2/v3, BGP4, BGP4+, OSPF multiple process, LPM Routing, Policy-based Routing (PBR) IPv4/IPv6, VRRP, IPv6 VRRPv3, URPF IPv4/IPv6, ECMP, BFD, Static Multicast Route, Multicast Receive Control, Illegal Multicast Source DetectAgregacja linków: IEEE 802.3ad (LACP), 64 groups per device / 8 ports per group, load balanceBezpieczeństwo: Storm Control based on packets, Port Security, MAC Limit based on VLAN and Port, Anti-ARP-Spoofing , Anti-ARP-Scan, ARP Binding, Gratuitous ARP, ARP Limit, Anti ARP/NDP Cheat, Anti ARP Scan, ND Snooping, DAI, IEEE 802.1x, Authentication, Authorization, Accounting, Radius IPv4/IPv6, TACACS+, MAB, Port and MAC based authentication, Accounting based on time length and traffic, Guest VLAN and auto VLAN,Multicast: IGMP v1/v2/v3 snooping and L2 Query, IGMP Fast leave, MVR, MLD v1/v2 Snooping, IPv4/IPv6 DCSCM, IGMP authenticationQoS: 8 queques per port, Bandwidth Control, Flow Control: HOL, IEEE802.3x, Flow Redirect, Classification based on ACL, COS, TOS, DiffServ, DSCP, port number; Traffic Policing, PRI Mark/Remark, IEEE 802.1p, Queuing Method: Strict Priority, Weighted Deficit Round Robin, Strict priority in Weighted Deficit Round Robin; DNS Client, DNS RelayLista Kontroli Dostępu: IP Src/Dst ACL, MAC Src/Dst ACL, MAC-IP ACL, User-Defined ACL, Time Range ACL, port number TCP/UDP ACL, VLAN ACL, REDIRECT and Statistics based on ACL, Vlan Tag/Untag, Rules can be configured to port and VLANDiagnostyka: sFlow, Traffic Analysis, VCT, Ping, Trace Route, Zarządzanie: TFTP/FTP, CLI, Telnet, Console, Web/SSL (IPv4/IPv6), SSH (IPv4/IPv6), SNMP v1/v2c/v3, SNMP Trap, Public & Private MIB interface, RMON 1,2,3,9, Syslog (IPv4/IPv6), SNTP/NTP (IPv4/IPv6), Dual IMG, Multiple Configuration Files, Port Mirror, IEEE 802.3ah OAM, ULDP (like UDLD), LLDP/LLDP MED., VSF (min. 4 devices in one stack) - hardware stacking |
| Oprogramowanie oraz wsparcie techniczne: | Oprogramowanie przełącznika (firmware) dostępne bez ograniczeń czasowych, przez cały okres cyklu życia urządzenia, poprzez Internet. Wymagane wsparcie techniczne producenta lub dystrybutora bez konieczności wykupu dodatkowych usług. |
| Wyposażenie | Wkładki kompatybilne z oferowanym rozwiązaniem 10Gbs 1310nm LC DDM SMF 10km (DFB+PIN) – 4 sztuki do każdego urządzenia |
| Gwarancja i serwis | Min. 5 lat (60 miesięcy) realizowane w trybie NBD (Next Business Day) obejmująca wymianę sprzętu na następny dzień roboczy oraz zapewnienie przez okres udzielonej gwarancji wsparcia technicznego realizowanego przez certyfikowanego inżyniera. Wsparcie musi być zapewnione od poniedziałku do piątku w godzinach 8:00-16:00 z możliwością realizacji zgłoszeń przez portal www lub e-mail, z maksymalnym czasem reakcji 3 dni na zgłoszone zagadnienie rozumiane jako diagnoza problemu, wsparcie przy optymalizacji konfiguracji etc. |

1. **Zakup zarządzalnych przełączników sieciowych - typ 2.**

|  |  |
| --- | --- |
| **Kryterium** | **Wymagane minimalne parametry lub funkcjonalności** |
| Typ | W ofercie wymagane jest podanie producenta, modelu/symbolu/nazwy handlowej, okresu gwarancji oraz wyposażenia. |
| Ilość | 2 zestawy |
| Wymagania techniczne i funkcjonalne | Porty przełącznika: minimum 20x 10/100/1000Base-T RJ45 wpierające PoE/PoE+, minimum 4x COMBO (10/100/1000Base-T RJ45 wspierające PoE/PoE+ lub 100/1000Base-X SFP) oraz minimum 4x 1/10GBase-X SFP+Port konsolowy: RJ45 (RS-232)Port zarządzania: RJ45 (10/100Base-T RJ45)Port USB: minimum 1 port co najmniej w standardzie 2.0Szybkość przełączania: minimum 128Gb/sPrzepustowość: minimum 95Mp/s (dla pakietów 64Kb)Bufor pakietów: minimum 1,5MBRamki Jumbo: minimum 10kTablica adresów MAC: minimum 16k Adresy MAC - Multicast: minimum 4kTablica ACL: minimum 3kTablica VLAN: minimum 4kTablica routingu: minimum 1k dla IPv4 z możliwością wykorzystania IPv6. Dopuszcza się rozwiązania współdzielące tablicę routingu dla IPv4 oraz IPv6 w maksymalnej proporcji 4:1.Pamięć Flash: minimum 32 MB + 128MB NANDPamięć RAM: minimum 512MBTemperatura pracy: zakres minimum 0°C - 50°CWilgotność względna: zakres minimum 10% - 90% (bez kondensacji)Obsługa technologii PoE: IEEE 802.3 af (15,4W), IEEE 802.3at (30W)Budżet mocy PoE: minimum 370WZasilanie: zabudowany zasilacz 230V ACPobór mocy: maksymalnie 471WZabezpieczenie przeciwprzepięciowe: minimum 4kVAlgorytm pracy: Store and ForwardObsługa VLAN: Voice VLAN, Port based VLAN, MAC based VLAN, Protocol based VLAN, Private VLAN, VLAN Translation, N:1 VLAN Translation, GVRP, IEEE 802.1Q, Normal QinQ, Flexible QinQDHCP: IPv4/IPv6 DHCP Client,IPv4/IPv6 DHCP Relay, Option 82, IPv4/IPv6 DHCP Snooping,IPv4/IPv6 DHCP ServerDrzewo rozpinające: IEEE802.1D (STP), IEEE802.1W (RSTP), IEEE802.1S (MSTP), Multi-Process MSTP, Root Guard, BPDU guard, BPDU forwarding, Protekcja ringowa: ITU-T G.8032 - recovery time < 50ms, Loopback Detection, Fast LinkProtokoły routingu: Static Routing, RIPv1/v2, RIPng, OSPFv2/v3, BGP4, BGP4+, OSPF multiple process, LPM Routing, Policy-based Routing (PBR) IPv4/IPv6, VRRP, IPv6 VRRPv3, URPF IPv4/IPv6, ECMP, BFD, Static Multicast Route, Multicast Receive Control, Illegal Multicast Source Detect, GRE TunnelAgregacja linków: IEEE 802.3ad (LACP), 128 groups per device / 8 ports per group, load balanceBezpieczeństwo: Storm Control based on packets, Port Security, MAC Limit based on VLAN and Port, Anti-ARP-Spoofing , Anti-ARP-Scan, ARP Binding, Gratuitous ARP, ARP Limit, Anti ARP/NDP Cheat, Anti ARP Scan, ND Snooping, DAI, IEEE 802.1x, Authentication, Authorization, Accounting, Radius IPv4/IPv6, TACACS+, MAB, Port and MAC based authentication, Accounting based on time length and traffic, Guest VLAN and auto VLAN,Multicast: IGMP v1/v2/v3 snooping and L2 Query, IGMP Fast leave, MVR, MLD v1/v2 Snooping, IPv4/IPv6 DCSCM, PIM-SM, PIM-DM, PIM-SSM, IGMP authenticationQoS: 8 queques per port, Bandwidth Control, Flow Control: HOL, IEEE802.3x, Flow Redirect, Classification based on ACL, COS, TOS, DiffServ, DSCP, port number; Traffic Policing, PRI Mark/Remark, IEEE 802.1p, Queuing Method: Strict Priority, Weighted Deficit Round Robin, Strict priority in Weighted Deficit Round Robin; DNS Client, DNS RelayLista Kontroli Dostępu: IP Src/Dst ACL, MAC Src/Dst ACL, MAC-IP ACL, User-Defined ACL, Time Range ACL, port number TCP/UDP ACL, VLAN ACL, REDIRECT and Statistics based on ACL, Standard and Expanded ACL based on IP Protocol and IP Precedence, Vlan Tag/Untag, Rules can be configured to port and VLANDiagnostyka: sFlow, Traffic Analysis, RSPAN, VCT, Ping, Trace Route, Dying GASPZarządzanie: TFTP/FTP, CLI, Telnet, Console, Web/SSL (IPv4/IPv6), SSH (IPv4/IPv6), SNMP v1/v2c/v3, SNMP Trap, Public & Private MIB interface, RMON 1,2,3,9, Syslog (IPv4/IPv6), SNTP/NTP (IPv4/IPv6), Dual IMG, Multiple Configuration Files, Port Mirror, IEEE 802.3ah OAM, ULDP (like UDLD), LLDP/LLDP MED, VSF (4 devices in one stack) - hardware stackingFunkcje PoE: Support IEEE 802.3at for all ports, PD failure detection, PoE scheduling |
| Oprogramowanie | Oprogramowanie przełącznika (firmware) dostępne bez ograniczeń czasowych, przez cały okres cyklu życia urządzenia, poprzez Internet. Wymagane wsparcie techniczne producenta lub dystrybutora bez konieczności wykupu dodatkowych usług. |
| Wyposażenie | Wkładki kompatybilne z oferowanym rozwiązaniem 10Gbs 1310nm LC DDM SMF 10km (DFB+PIN) – 4 sztuki do każdego urządzenia |
| Gwarancja i serwis | Min. 5 lat (60 miesięcy) realizowane w trybie NBD (Next Business Day) obejmująca wymianę sprzętu na następny dzień roboczy oraz zapewnienie przez okres udzielonej gwarancji wsparcia technicznego realizowanego przez certyfikowanego inżyniera. Wsparcie musi być zapewnione od poniedziałku do piątku w godzinach 8:00-16:00 z możliwością realizacji zgłoszeń przez portal www lub e-mail, z maksymalnym czasem reakcji 3 dni na zgłoszone zagadnienie rozumiane jako diagnoza problemu, wsparcie przy optymalizacji konfiguracji etc. |

1. **Zakup zasilaczy awaryjnych UPS typu Rack - typ 2.**

|  |  |
| --- | --- |
| **Kryterium** | **Wymagane minimalne parametry lub funkcjonalności** |
| Typ | W ofercie wymagane jest podanie producenta, modelu/symbolu/nazwy handlowej, okresu gwarancji oraz wyposażenia. |
| Ilość | 3 zestawy |
| Wymagania techniczne i funkcjonalne | Obudowa Rack max 1UMoc 1500VAKształt fali wyjściowej: pełna fala sinusoidalna4 gniazda wyjściowe  |
| Wyposażenie | Elementy montażowe pozwalające na instalację zasilacza w szafie Rack.Listwa zasilająca do montażu w szafie Rack, 8 gniazd, przewód umożliwiający wpięcie do zasilacza UPS. |
| Gwarancja i serwis | Min. 2 lata (24 miesiące) |

1. **Zakup systemu DLP ze wsparciem w okresie trwania projektu.**

|  |  |
| --- | --- |
| **Kryterium** | **Wymagane minimalne parametry lub funkcjonalności** |
| Typ | W ofercie wymagane jest podanie pełnej nazwy handlowej systemu, typu licencji, liczby użytkowników, okresu wsparcia technicznego , okresu gwarancji. |
| Ilość | 1 zestaw |
| Typ licencji | Licencja wieczysta z odnawialnym wsparciem technicznym dla 70 użytkowników |
| Wymagania techniczne i funkcjonalne | * + - 1. Serwer administracyjny musi obsługiwać instalację na systemach: Windows Server 2016 (64-bit) i nowszych.
			2. Serwer administracyjny musi obsługiwać bazy danych:
				1. MS SQL Server 2016 lub nowsze,
				2. MS SQL Express,
				3. AzureSQL S3 lub nowsze.
			3. Konsola administracyjna i komunikaty klienta muszą być w języku polskim.
			4. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
			5. Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na stacjach roboczych.
			6. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym.
			7. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia.
			8. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli.
			9. System musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych, usuwając najstarsze informacje, gdy rozmiar bazy osiągnie skonfigurowany limit.
			10. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania.
			11. Administrator musi mieć możliwość aby tworzyć, usuwać i konta administratorów w konsoli programu.
			12. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu).
			13. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory.
			14. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą, a serwerem w czasie rzeczywistym.
			15. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa.
			16. Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości email oraz czynności na plikach.
			17. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików.
			18. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych.
			19. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email.
			20. Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu.
			21. Serwer administracyjny musi posiadać wbudowany serwer SMTP dostarczony przez producenta oprogramowania.
			22. Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak i nowo powstałych na bazie już skategoryzowanych plików.
			23. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku.
			24. Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami itp.
			25. Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer paszportu, wyrażenia regularne, określone ciągi znaków i numer IBAN.
			26. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
			27. Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM.
			28. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP.
			29. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwiać aktualizację do nowej wersji lub dezaktywację tego oprogramowania.
			30. System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysyłaną przez użytkowników Microsoft 365.
			31. System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams.
			32. System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach
			33. System musi posiadać możliwość integracji z systemami do analizy danych (PowerBI, Tableau, etc.)
			34. System musi zapewniać możliwość zarządzanie szyfrowaniem dysków twardych oraz urządzeń wymiennych.
 |
| Okres ochrony | Licencje oraz serwisy powinny mieć zapewnione aktualizację oraz wsparcie techniczne w okresie realizacji projektu do 30.06.2026 r. |
| Usługa asysty wdrożeniowej | Obowiązkiem Zamawiającego będzie zapewnienie usługi asysty wdrożeniowej w następującym zakresie:1. Instalacja i konfiguracja serwera Safetica - oprogramowania zarządzającego.
2. Przygotowanie procedury instalacyjnej klientów oraz instalacja klientów na stacjach roboczych.
3. Integracja z Active Directory.
4. Włączenie funkcji audytowania i podstawowa analiza wycieków danych z jednej przykładowej stacji.
5. Wygenerowanie przykładowego raportu.
6. Omówienie funkcji konsoli.
7. Wdrożenie kontroli dostępu do stron WWW.
8. Ustawienie klasyfikacji danych w oparciu o wskazane przez klienta dane wrażliwe.
9. Utworzenie maksymalnie trzech polityk DLP (np. pochodzenia pliku, zawartości pliku, właściwości pliku).
 |
| Gwarancja i serwis | Min. 2 lata (24 miesiące) |