- **Serwer NAS – 1 szt.**

Opis oraz minimalne wymagania techniczne Zamawiającego
1. **Jednostka centralna (CPU):** Architektura x86-64, wyposażona w minimum 4 rdzeni fizycznych o taktowaniu nie mniejszym niż 2.0 GHz.
2. **Pamięć RAM:** Minimum 8 GB DDR4. Płyta główna musi posiadać co najmniej 2 sloty na pamięć z możliwością rozbudowy do min. 64 GB. Zalecana obsługa korekcji błędów ECC.
3. **Pamięć systemowa (Flash):** Dedykowany moduł lub dysk na system operacyjny o pojemności min. 4 GB.
4. **Zatoki i dyski HDD:** Obudowa wyposażona w min. 8 zatok 3.5" SATA z Hot-Swap. Zainstalowane 3 dyski HDD o poj. min. 8 TB każdy (7200 obr/min), wykonane w technologii CMR, do pracy ciągłej.
5. **Kontroler pamięci masowej:** Możliwość pracy w trybie IT / HBA (Direct Pass-through), zapewniająca systemowi operacyjnemu bezpośredni dostęp do dysków (wymóg dla stabilności ZFS).
6. **Interfejsy sieciowe:** Minimum 2 porty LAN 2,5 Gb/s (RJ-45) oraz minimum 2 porty LAN 10 Gb/s (złącza SFP+).
7. **Porty i rozbudowa:** Minimum 3 porty USB 3.2 Gen 2 oraz minimum 2 wolne złącza PCIe umożliwiające dalszą rozbudowę urządzenia.
8. **Zarządzanie danymi (RAID/ZFS):** Obsługa poziomów RAID 0, 1, 5, 6, 10 oraz odpowiedników ZFS (RAID-Z1, RAID-Z2, Mirror). Możliwość rozszerzania pojemności i migracji poziomów online.
9. **Ochrona danych i Snapshoty:** Obsługa nielimitowanych migawek (Snapshots), samo naprawa danych (Self-healing) oraz obsługa iSCSI (Target/Initiator) z MPIO.
10. **Usługi sieciowe i Backup:** Obsługa protokołów SMB (v1-v3), NFS, FTP, SFTP oraz natywna synchronizacja z chmurami: Google Drive, Dropbox, OneDrive.
11. **Wirtualizacja i Kontenery:** Możliwość uruchamiania kontenerów (Docker, LXC lub Jails) oraz pełnych maszyn wirtualnych (KVM, Bhyve lub równoważne).
12. **Bezpieczeństwo i Dostęp:** Szyfrowanie wolumenów AES-256, integracja z Windows AD / LDAP, obsługa list kontroli dostępu Windows ACL.
13. **Administracja i Monitoring:** Zarządzanie przez GUI (WWW) oraz SSH. Obsługa SNMP (v2/v3), powiadomienia E-mail/SMS oraz współpraca z UPS (USB/SNMP/ Network).
14. **Warunki pracy i obudowa:** Dopuszczalna temperatura pracy 0-40˚C, wilgotność do 95%. Przyciski: Power, Reset. Diody: Status, LAN, HDD.
15. **Gwarancja i wsparcie:** Minimum 36 miesięcy (3 lata) gwarancji producenta lub dostawcy.

- **Switch zarządzalny L2/L3 (24 porty) – 3 szt.**

Opis oraz minimalne wymagania techniczne Zamawiającego
1. Charakterystyka portów: Minimum 24 porty RJ-45 10/100/1000Mb/s Base-T zgodne z IEEE 802.3i/u/ab oraz minimum 2 porty SFP+ o przepustowości 10Gb zgodne z IEEE 802.3ae.
2. Funkcje Warstwy 3 (L3): Obsługa routingu statycznego, wpisów statycznych ARP oraz Proxy ARP. Wbudowany serwer DHCP oraz obsługa DHCP Relay (Interface, VLAN, L2).
3. Protokoły L2 i redundancja: Obsługa agregacji połączeń LACP (802.3ad), protokołów drzewa rozpinającego STP (802.1D), RSTP (802.1w), MSTP (802.1s) oraz kontroli przepływu 802.3x.
4. Zarządzanie ruchem Multicast: Obsługa IGMP Snooping (v1/v2/v3), funkcji Fast Leave, IGMP Snooping Querier oraz uwierzytelniania IGMP.
5. Sieci VLAN: Obsługa tagowania 802.1Q VLAN, protokołu GVRP oraz QinQ (oparty na portach i Selective QinQ).
6. Listy Kontroli Dostępu (ACL): Rozbudowane ACL oparte na adresach MAC (źródłowy/docelowy, VLAN ID, Ethertype) oraz adresach IP (źródłowy /docelowy, protokół, flagi TCP, porty TCP/UDP, DSCP/IP). Możliwość przypisania ACL do portu i VLAN.
7. Bezpieczeństwo i Autoryzacja: Obsługa 802.1X (na port i MAC), MAB (MAC Authentication Bypass), Guest VLAN, uwierzytelnianie Radius/TACACS+ (AAA) oraz izolacja portów.
8. Jakość usług (QoS) i wydajność: Minimum 6 kolejek priorytetowania, obsługa 802.1p. Tablica adresów MAC min. 16k, obsługa ramek Jumbo do 9KB.
9. Zarządzanie i administracja: Dostęp przez interfejs graficzny GUI, linię poleceń CLI oraz SNMP v1/v2c/v3. Możliwość zarządzania w chmurze.
10. Konstrukcja i zasilanie: Obudowa z elementami montażowymi do szafy rack 19", zasilanie 230V 50Hz, certyfikat CE.
11. Gwarancja: Minimum 36 miesięcy gwarancji producenta z zapewnieniem wsparcia i aktualizacji oprogramowania w tym okresie.

- **Switch zarządzalny L2/L3 (48 portów) – 2 szt.**

Opis oraz minimalne wymagania techniczne Zamawiającego
1. Charakterystyka portów: Minimum 48 portów RJ-45 10/100/1000Mb/s Base-T zgodne z IEEE 802.3i/u/ab oraz minimum 2 porty SFP+ o przepustowości 10Gb zgodne z IEEE 802.3ae.
2. Funkcje Warstwy 3 (L3): Obsługa routingu statycznego, wpisów statycznych ARP oraz Proxy ARP. Wbudowany serwer DHCP oraz obsługa DHCP Relay (Interface, VLAN, L2).
3. Protokoły L2 i redundancja: LACP (802.3ad), STP (802.1D), RSTP (802.1w), MSTP (802.1s) oraz kontrola przepływu 802.3x. Port Mirroring.

Opis oraz minimalne wymagania techniczne Zamawiającego
4. Zarządzanie ruchem Multicast: Obsługa IGMP Snooping (v1/v2/v3), Fast Leave, IGMP Snooping Querier oraz uwierzytelniania IGMP.
5. Sieci VLAN: Tagowanie 802.1Q VLAN, GVRP, QinQ oparty na portach oraz Selective QinQ.
6. Listy Kontroli Dostępu (ACL): Pełna filtracja L2-L4: MAC ACL (źródło/cel, VLAN, Ethertype) oraz IP ACL (źródło/cel, protokół, porty TCP/UDP, DSCP).
7. Bezpieczeństwo i Autoryzacja: Uwierzytelnianie 802.1X, MAB, Guest VLAN, Radius/TACACS+ (AAA) oraz izolacja portów.
8. Jakość usług (QoS) i wydajność: Minimum 6 kolejek priorytetowania, obsługa 802.1p. Tablica adresów MAC min. 16k, obsługa ramek Jumbo do 9KB.
9. Zarządzanie i administracja: Interfejs GUI, CLI, SNMP v1/v2c/v3. Możliwość zarządzania w chmurze.
10. Konstrukcja i zasilanie: Obudowa rack 19", zasilanie 230V 50Hz, certyfikat CE.
11. Gwarancja: Minimum 36 miesięcy gwarancji producenta z aktualizacjami i wsparciem.

- **System klasy SIEM z repozytorium zdarzeń – 1 kp**

Opis oraz minimalne wymagania techniczne Zamawiającego
1. Zakres i licencjonowanie: Dostawa i wdrożenie systemu SIEM dla min. 40 urządzeń końcowych (stacji/serwerów). System musi działać na licencji otwartej (możliwość modyfikacji kodu, dopisywania modułów, brak limitów na własne reguły).
2. Architektura i składowanie: Instalacja lokalna (on-premise) z dedykowanym repozytorium logów na serwerze Zamawiającego. System musi zapewniać centralną kolekcję, archiwizację i retencję danych zgodnie z regulacjami Urzędu.
3. Funkcjonalność analityczna: Korelacja zdarzeń w czasie rzeczywistym, wykrywanie anomalii i prób włamań. Mechanizmy automatycznych powiadomień o incydentach oraz dashboardy/raporty wizualne.
4. Agenci i monitoring: Możliwość instalacji agentów na systemach Windows i Linux. Pełny monitoring stacji roboczych, serwerów i urządzeń sieciowych.
5. Integracje systemowe: Konfiguracja integracji z: Firewall Fortigate (logi ruchu), Serwerami Windows (AD, usługi aplikacyjne), Agregatem prądotwórczym oraz zasilaczami UPS. Możliwość ręcznego dopisywania integratorów.
6. Wdrożenie i prace inżynierskie: Realizacja min. 90 godzin prac wdrożeniowych na miejscu (instalacja, konfiguracja, integracje, tworzenie reguł i dashboardów, testy, dokumentacja powykonawcza).
7. Szkolenie administratorów: Przeprowadzenie pełnego szkolenia dla personelu Zamawiającego w zakresie obsługi i administracji systemem.

Opis oraz minimalne wymagania techniczne Zamawiającego
8. Wsparcie techniczne i SLA: Minimum 24 miesiące wsparcia technicznego obejmującego aktualizacje, pomoc w tworzeniu reguł i raportów oraz konsultacje. Czas reakcji do 2h
9. Wymagania niefunkcjonalne: Praca wyłącznie w sieci lokalnej (zakaz usług chmurowych), dostęp przez przeglądarkę WWW, pełna kompatybilność z używanymi systemami operacyjnymi.

- **Audyty wraz z dokumentacją SZBI – 1 szt.**

Opis oraz minimalne wymagania techniczne Zamawiającego
1. Audyt początkowy: Przeprowadzenie audytu stanu bezpieczeństwa informacji w UG oraz jednostkach podległych.
2. Dokumentacja SZBI dla Urzędu i 2 jednostek podległych – Polityki: Opracowanie i wdrożenie: • Polityka zarządzania systemem informatycznym • Polityka bezpieczeństwa informacji • Polityka zapewnienia ciągłości działania • Polityka ochrony danych osobowych • Polityka bezpieczeństwa dotycząca dostawców (w tym klauzule bezpieczeństwa) • Polityka bezpiecznego rozwoju systemów (w tym specyfikacja wymagań). **Rejestry i Analizy:** Opracowanie i wdrożenie: • Rejestr aktywów wraz z Polityką akceptowalnego użytkowania aktywów • Polityka kontroli dostępu i zarządzania hasłami • Procedura zarządzania incydentami cyberbezpieczeństwa • Analiza ryzyka w obszarze bezpieczeństwa informacji. **Procedury operacyjne SZBI:** Opracowanie i wdrożenie procedur zgodnych z prawem: • Procedury przesyłania informacji i bezpiecznej komunikacji • Plan reagowania na incydenty i procedury ich obsługi • Polityka czystego ekranu i czystego biurka • Procedury ochrony logów systemowych i zarządzania podatnościami • Plany przywracania działania systemów (Disaster Recovery) • Realizacja i weryfikacja kopii zapasowych • Procedury pracy zdalnej i korzystania z urządzeń mobilnych • Zarządzanie bezpieczeństwem sieci i kontrola dostępu • Zabezpieczenia fizyczne pomieszczeń i obiektów • Postępowanie z nośnikami danych. **Zgodność prawna i szkolenia:** • Procedura identyfikacji wymagań prawnych wraz z Wykazem wymagań • Program szkoleń z zakresu bezpieczeństwa informacji dla personelu • Przeszkolenie pracowników z wdrożonej dokumentacji SZBI.
3. Audyt Końcowy: Przeprowadzenie audytu końcowego w Urzędzie Gminy i 2 jednostkach podległych, potwierdzającego zgodność z normą **ISO 27001 oraz KRI**.

- **Szkolenia z zakresu cyberbezpieczeństwa oraz Voucher – 1 szt.**

Opis oraz minimalne wymagania techniczne Zamawiającego
1. Szkolenie dla pracowników (Cyberbezpieczny Samorząd): Szkolenie stacjonarne (min. 6h dydaktycznych) realizowane dla grup liczących maksymalnie 30 uczestników. Zakres merytoryczny szkolenia powinien obejmować co najmniej następujące obszary tematyczne:

Opis oraz minimalne wymagania techniczne Zamawiającego
• Wprowadzenie do cyberbezpieczeństwa, • Zagrożenia: phishing, ransomware, socjotechnika, • Bezpieczna poczta, przeglądarki i nośniki danych, • Silne hasła i uwierzytelnianie wieloskładnikowe (MFA), • Ochrona danych osobowych w IT, • Dobre praktyki w pracy urzędnika.
2. Szkolenie dla Kadry Zarządzającej: Szkolenie stacjonarne (min. 6h). Zakres jak dla pracowników, rozszerzony o: • Zarządzanie bezpieczeństwem wg zaleceń KSC i KRI, • Elementy Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). **Zaplecze szkoleniowe:** Wykonawca zapewnia: • Materiały szkoleniowe (drukowane lub cyfrowe), • Listy obecności, • Imienne zaświadczenia/certyfikaty ukończenia szkolenia dla uczestników. **Wymagania wobec Trenera:** • Doświadczenie w prowadzeniu szkoleń z cyberbezpieczeństwa, w szczególności realizowanych dla jednostek samorządu terytorialnego. • Znajomość specyfiki środowiska administracji publicznej, • Umiejętność skutecznego przekazywania wiedzy osobom nietechnicznym.
3. Voucher specjalistyczny: Przekazanie vouchera dla jednej osoby na szkolenie: „Audytor wewnętrzny ISO 27001" z terminem ważności nie krótszym niż do dnia 31 grudnia 2026 r., lub przeprowadzanie wskazanego szkolenie w terminie nie późniejszym niż do dnia 1 czerwca 2026 r.

- **Testy penetracyjne i socjotechniczne (Phishing/Vishing)**

Opis oraz minimalne wymagania techniczne Zamawiającego
1. Testy penetracyjne infrastruktury: Ocena bezpieczeństwa obejmująca: • Testy zewnętrzne (publiczne IP, usługi sieciowe), • Testy wewnętrzne (LAN/WLAN, serwery, stacje robocze), • Analizę konfiguracji urządzeń sieciowych i usług. Prace prowadzone w oknach czasowych niezakłócających pracy Urzędu.
2. Kampania phishingowa (e-mail): Kontrolowana kampania socjotechniczna: • Przygotowanie e-maili imitujących wyłudzenia, • Wysyłka do grup pracowników i monitoring wskaźników (otwarcia, kliknięcia, podanie danych), • Anonimizacja danych zgodnie z RODO, • Zakaz użycia malware/ransomware. Po testach – informacja zwrotna i materiały edukacyjne dla pracowników.
3. Testy telefoniczne (Vishing): Symulowane próby pozyskania informacji drogą telefoniczną w celu oceny reakcji pracowników i odporności na manipulację.
4. Raport końcowy z testów: Dokument musi zawierać: • Podsumowanie z oceną ryzyka, • Wykaz podatności z priorytetyzacją, • Wnioski procesowe i zalecenia naprawcze, • Statystyki kampanii phishingowej (zgodne z RODO), • Materiały dedykowane dla kierownictwa i działu IT.

Opis oraz minimalne wymagania techniczne Zamawiającego
5. Wymagania wobec Wykonawcy: • Posiadanie aktualnego ubezpieczenia OC, • Działanie zgodne z prawem i zasadami etyki testów bezpieczeństwa.