

Fundusze Europejskie
na Rozwój CyfrowyRzeczpospolita
PolskaDofinansowane przez
Unię EuropejskąCENTRUM
PROJEKTÓW
POLSKA
CYFROWA

• **Serwer wraz z oprogramowaniem – 1 szt.**

Opis oraz minimalne wymagania techniczne Zamawiającego
1. Płyta główna: zaprojektowana przez producenta serwera, min. 4 sloty RAM, moduł TPM min. 2.0 zainstalowana w obudowie RACK wraz z szynami montażowymi.
2. Procesor: min. 4 rdzeni fizyczne, min. 2.80 GHz, wynik Passmark min. 10000 pkt dla multicore.
3. Pamięć RAM: min. 16 GB DDR5 UDIMM ECC min. 5600MT/s (podać liczbę wolnych slotów - min. 2).
4. Kontroler dyskowy: sprzętowy z obsługą RAID 0, 1,10. Możliwość obsługi minimum 4 dysków 2,5" lub 3,5" poprzez kieszenie w obudowie serwera.
5. Dyski twarde: 2x min. 960 GB przeznaczone do pracy ciągłej w zastosowaniach serwerowych.
6. Karty sieciowe: 2x 1000Base-T
7. Zarządzanie: karta zarządzająca z dedykowanym portem RJ-45.
8. System operacyjny: min. Microsoft Windows Server 2025 Standard (4 Core) lub równoważny zapewniający obsługę Active Directory lub równoważnych rozwiązań kompatybilnych z infrastrukturą zamawiającego.
9. Licencje CAL: 35 szt. Device CAL 2025 oraz 1 szt. RDS User CAL 2025 lub równoważne.
10. Gwarancja: Min. 2 lata gwarancji producenta. Zgłoszenia przez kanał komunikacji producenta.
11. Warunki serwisu: Pozostawienie uszkodzonych dysków u zamawiającego.

• **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 2.2 GHz.
2. Pamięć RAM: Minimum 4 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)
7. Porty i rozbudowa: Minimum 3 porty USB 3.2 Gen 2 oraz minimum 1 wolne złącza PCIe umożliwiające dalszą rozbudowę urządzenia.



Fundusze Europejskie
na Rozwój CyfrowyRzeczpospolita
PolskaDofinansowane przez
Unię Europejską

Opis oraz minimalne wymagania techniczne Zamawiającego	
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), 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 24 miesiące (2 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:	



Fundusze Europejskie
na Rozwój CyfrowyRzeczpospolita
PolskaDofinansowane przez
Unię EuropejskąCENTRUM
PROJEKTÓW
POLSKA
CYFROWA

Opis oraz minimalne wymagania techniczne Zamawiającego
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 24 miesiące 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.
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 24 miesiące gwarancji producenta z aktualizacjami i wsparciem.



Fundusze Europejskie
na Rozwój CyfrowyRzeczpospolita
PolskaDofinansowane przez
Unię EuropejskąCENTRUM
PROJEKTÓW
POLSKA
CYFROWA

• **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.
8. Wsparcie techniczne i SLA: Minimum 12 miesięcy wsparcia technicznego obejmującego aktualizacje. 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 wraz z obszarem wodociągów.
2. Dokumentacja SZBI dla Urzędu wraz z lokalizacją rezerwową UG i 2 jednostek podległych i wodociągów– 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 użytkownika aktywów • Polityka kontroli dostępu i zarządzania hasłami • Procedura zarządzania incydentami cyberbezpieczeństwa



Fundusze Europejskie
na Rozwój CyfrowyRzeczpospolita
PolskaDofinansowane przez
Unię EuropejskąCENTRUM
PROJEKTÓW
POLSKA
CYFROWA**Opis oraz minimalne wymagania techniczne Zamawiającego**

- 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.
- Procedura przeniesienia do jednostki rezerwowej.

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 wraz z infrastrukturą wodociągową oraz lokalizacji rezerwowej dla UG i 2 jednostkach podległych, potwierdzającego zgodność z normą **ISO 27001 oraz KRI i KSC**.

- **Szkolenia z zakresu cyberbezpieczeństwa**

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:

- 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 minimum przeprowadzone 4 szkoleń dla JST.
- Znajomość specyfiki środowiska administracji publicznej,
- Umiejętność skutecznego przekazywania wiedzy osobom nietechnicznym.

3. Realizacja specjalistycznego szkolenia mającego na celu przygotowanie pracownika jednostki samorządu terytorialnego (JST) do **pełnienia funkcji audytora wewnętrznego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnego z normą PN-EN ISO/IEC 27001**. Szkolenie ma charakter ekspercki i koncentruje się na przekazaniu wiedzy oraz rozwinięciu praktycznych kompetencji umożliwiających samodzielne planowanie, przeprowadzanie oraz dokumentowanie audytów wewnętrznych SZBI w jednostkach samorządu terytorialnego. W ramach projektu „Cyberbezpieczny Samorząd”

Cyberbezpieczny
Samorząd

**Opis oraz minimalne wymagania techniczne Zamawiającego**

Szkolenie powinno obejmować: Podstawy bezpieczeństwa informacji i SZBI: znaczenie bezpieczeństwa informacji w administracji publicznej, cele i zasady funkcjonowania SZBI, role i odpowiedzialność kierownictwa oraz audytorów. Norma PN-EN ISO/IEC 27001: struktura normy i jej kluczowe wymagania, kontekst organizacji oraz podejście oparte na analizie ryzyka, Załącznik A – cele oraz środki kontroli bezpieczeństwa. Audyt wewnętrzny – podstawy metodyczne: definicja i cele audytu wewnętrznego, rodzaje audytów, kompetencje oraz zasady etyki audytora. Wytyczne dotyczące audytowania systemów zarządzania: zasady audytowania systemów zarządzania, planowanie programu audytów oraz przygotowanie audytu. Realizacja audytu wewnętrznego SZBI: prowadzenie spotkań otwierających i zamykających, techniki zbierania dowodów audytowych (wywiady, obserwacje, analiza dokumentacji), identyfikowanie niezgodności i formułowanie obserwacji. Raportowanie i działania poaudytowe: przygotowanie raportu z audytu, formułowanie niezgodności oraz rekomendacji, monitorowanie realizacji działań korygujących. Audyty SZBI w JST – aspekty praktyczne: specyfika prowadzenia audytów w jednostkach samorządu terytorialnego, najczęściej występujące niezgodności i problemy, dobre praktyki w audytowaniu. Warsztaty praktyczne: symulacja audytu wewnętrznego SZBI, analiza studiów przypadków, ćwiczenia z przygotowywania ustaleń audytowych. Szkolenie stacjonarne – zamawiający nie zapewnia sali szkoleniowej, szkolenie powinno się odbyć w odległości maksymalnie 25km od siedziby zamawiającego. Czas trwania minimum 3 dni szkoleniowe: od 6 do 8 godzin dydaktycznych. Wykonawca zapewni: materiały szkoleniowe (drukowane lub cyfrowe), listę obecności, certyfikaty ukończenia szkolenia.

• **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 (zgodnie z RODO),
- Materiały dedykowane dla kierownictwa i działu IT.

5. Wymagania wobec Wykonawcy:

- Posiadanie aktualnego ubezpieczenia OC,
- Działanie zgodne z prawem i zasadami etyki testów bezpieczeństwa.

