

Załącznik nr 1 do SWZ

Szczegółowy opis przedmiotu zamówienia.**Uwagi:**

1. Szkolenia muszą być dostosowane do wymogów standardów dostępności dla polityki spójności 2021-2027. Standardy można znaleźć w postaci załącznika na stronie (załącznik nr 2 w sekcji „Załączniki”):

<https://www.funduszeuropejskie.gov.pl/strony/o-funduszach/dokumenty/wytyczne-dotyczace-realizacji-zasad-rownosciowych-w-ramach-funduszy-unijnych-na-lata-2021-2027-1/>

W szczególności:

- a. dostosowania realizacji szkolenia (patrz → Standard szkoleniowy (szkolenia, kursy, warsztaty) → Rozdział 3)
 - b. dostosowania materiałów i informacji pisanej (patrz → Standard informacyjno-promocyjny → Rozdział 3)
 - c. dostosowania materiałów i informacji elektronicznej (patrz → Standard informacyjno-promocyjny → Rozdział 4)
 - d. dostosowania dokumentów elektronicznych (patrz → Standard cyfrowy → Rozdział 3)
2. Szkolenie na miejscu dla pracowników Urzędu Miasta. Minimum 3 trenerów.
 3. Wykonawca najpóźniej w dniu podpisania umowy zobowiązany będzie do zapoznania się z wewnętrznymi procedurami dokonywania zgłoszeń naruszeń prawa i podejmowania działań następczych w Urzędzie Miasta Biała Podlaska zamieszczonych w Biuletynie Informacji Publicznej link: <https://umbialapodlaska.bip.lubelskie.pl/index.php?id=1059>
 4. Oświadczamy, że szkolenia z cyberbezpieczeństwa w ramach projektu Cyberbezpieczny Samorząd są w całości finansowane ze środków publicznych. Zgodnie z treścią art. 43 ust. 1. pkt 29 lit. c ustawy z dnia 11 marca 2004 roku o podatku od towarów i usług (Dz. U. Nr 54, poz 535 ze zm.) proszę o składanie oferty ze stawką VAT zwolnioną.

Szkolenie na miejscu, minimum trzydniowe zgodnie z planem szkolenia.

Temat: Bezpieczeństwo informacji w świetle NIS2, ISO 27001, ISO 22301 oraz specyfiki administracji publicznej

Grupa docelowa: Pracownicy urzędu miasta, w tym osoby odpowiedzialne za przetwarzanie danych, zarządzanie systemami informatycznymi, bezpieczeństwo informacji oraz kierownictwo

1. Podstawy bezpieczeństwa informacji i specyfika pracy urzędów

1. Wprowadzenie do bezpieczeństwa informacji w administracji publicznej

- Kluczowe pojęcia: ochrona danych osobowych, bezpieczeństwo informacji, cyberbezpieczeństwo
- Specyficzne zagrożenia w pracy urzędów miasta: phishing, ransomware, błędy ludzkie
- Przykłady incydentów w administracji i ich skutki

2. Regulacje prawne dotyczące bezpieczeństwa informacji w administracji publicznej

- RODO i jego wpływ na procesy w urzędzie
- Dyrektywa NIS2 i jej zastosowanie w administracji publicznej
- Ustawa o ochronie danych osobowych w praktyce urzędowej

3. Bezpieczna praca z danymi w urzędzie

- Ochrona danych osobowych w codziennej pracy urzędu
- Zarządzanie dostępem do systemów informatycznych
- Bezpieczne przechowywanie i niszczenie dokumentów papierowych i elektronicznych

4. Budowanie świadomości cyberzagrożeń

- Typowe oszustwa, na które narażeni są pracownicy urzędów
- Jak rozpoznawać podejrzane e-maile i linki?
- Warsztat: Analiza fałszywych wiadomości i phishingu

2. Zarządzanie ryzykiem i Dyrektywa NIS2 w praktyce urzędowej

1. Zarządzanie ryzykiem w urzędach miasta

- Identyfikacja ryzyk związanych z bezpieczeństwem informacji
- Tworzenie katalogu zagrożeń dla urzędów
- Warsztat: Analiza ryzyka na przykładzie wydziału ewidencji ludności

2. Dyrektywa NIS2 w administracji publicznej

- Kluczowe obowiązki urzędów wynikające z NIS2
- Zarządzanie incydentami i zgłaszanie ich do CSIRT GOV
- Przykłady wdrożeń w jednostkach administracji publicznej

3. Tworzenie polityk bezpieczeństwa w urzędzie miasta

- Elementy Polityki Bezpieczeństwa Informacji (PBI) dla urzędów
- Zarządzanie dostępem do informacji niejawnych i danych publicznych
- Przykładowe zapisy polityk dla administracji

4. Warsztat: Tworzenie procedur bezpieczeństwa w urzędzie

- Praca grupowa: Opracowanie procedur na wypadek incydentu bezpieczeństwa

3. ISO 27001 i zarządzanie ciągłością działania w urzędzie

1. System Zarządzania Bezpieczeństwem Informacji (ISO 27001)

- Struktura ISO 27001 i jej zastosowanie w urzędzie
- Wymagania dotyczące zabezpieczeń technicznych i organizacyjnych
- Proces certyfikacji w administracji publicznej

2. Zarządzanie ciągłością działania w urzędzie (ISO 22301)

- Tworzenie Planu Ciągłości Działania (PCD) dla urzędu miasta
- Analiza wpływu na działalność (BIA) w kontekście administracji publicznej
- Testowanie planów ciągłości działania

3. Bezpieczeństwo techniczne w systemach urzędowych

- Zabezpieczenia infrastruktury IT (LAN, Wi-Fi, serwery)
- Ochrona danych w chmurze i systemach on-premises
- Warsztat: Tworzenie listy wymagań dla systemów IT w urzędzie

4. Audytowanie i monitorowanie bezpieczeństwa

- Rola audytów w urzędach miasta
- Jak przygotować urząd do kontroli zewnętrznej?
- Warsztat: Opracowanie harmonogramu audytów wewnętrznych

4. Warsztaty praktyczne i wdrażanie dobrych praktyk

1. Zarządzanie incydentami bezpieczeństwa w urzędach

- Jak skutecznie reagować na incydenty?
- Przykłady incydentów i ich analiza
- Narzędzia wspierające zarządzanie incydentami

2. Budowanie kultury bezpieczeństwa w urzędzie miasta

- Szkolenia i kampanie dla pracowników urzędu
- Jak przekonać pracowników do przestrzegania zasad bezpieczeństwa?
- Warsztat: Tworzenie planu szkoleniowego dla urzędu

3. Warsztaty praktyczne – analiza przypadku

- Zespołowa analiza scenariusza cyberataku na urząd miasta
- Tworzenie planu działania i procedur zabezpieczających
- Symulacja zgłoszenia incydentu do CSIRT

4. Podsumowanie szkolenia

- Kluczowe wnioski i rekomendacje
- Dyskusja z uczestnikami: identyfikacja wyzwań w pracy urzędów
- Wręczenie certyfikatów uczestnictwa

Rezultaty szkolenia:

- Praktyczna wiedza o bezpieczeństwie informacji w pracy urzędu
- Umiejętność identyfikacji ryzyk i reagowania na incydenty
- Przygotowanie do wdrażania NIS2, ISO 27001 oraz ISO 22301 w administracji publicznej
- Zwiększenie świadomości pracowników w zakresie cyberbezpieczeństwa

Materiały szkoleniowe:

- Prezentacje, check-listy, przykładowe procedury
- Scenariusze incydentów i plany działania
- Lista kontrolna zgodności z NIS2 i ISO 27001 dla urzędów miasta

Szkolenie specjalistyczne dla IT. Na miejscu, minimum 3 dniowe. Zgodnie z planem szkolenia.

Zaawansowane szkolenie z konfiguracji i zabezpieczeń urządzeń FortiGate**1. Wprowadzenie do FortiGate i architektury systemu**

- Rola FortiGate jako NGFW (Next-Generation Firewall) i UTM
- Architektura FortiOS – funkcje systemu i ich moduły
- Tryby pracy FortiGate: NAT Mode a Transparent Mode
- Integracja jako firewall brzegowy / wewnętrzny / SD-WAN
- Przegląd sprzętu i wersji wirtualnych FortiGate VM
- Licencjonowanie i aktualizacje systemu FortiOS

2. Instalacja i podstawowa konfiguracja urządzenia

- Pierwsza konfiguracja GUI / CLI (console, SSH, web)
- Konfiguracja interfejsów sieciowych (Static / DHCP / PPPoE)
- Ustawienia DNS, NTP i synchronizacja czasu
- Zarządzanie użytkownikami i rolami administratora

- Tworzenie kopii zapasowych konfiguracji (TFTP, USB, cloud)
- Przywracanie systemu po awarii – factory reset, firmware recovery
- Diagnostyka CLI: get system status, diag sys top, diag sys session list

3. Konfiguracja firewall i polityk bezpieczeństwa

- Polityki Firewall Policy:
 - Omówienie Implicit Deny
 - Tworzenie reguł dostępu (IPv4, IPv6)
- Wdrożenie Deep Packet Inspection (DPI)
- NAT w FortiGate:
 - Source NAT (SNAT) – dynamiczny, statyczny
 - Destination NAT (DNAT) – Virtual IP (VIP)
 - Policy-Based NAT a Central NAT
- Traffic Shaping (QoS) – priorytetyzacja ruchu

4. Ochrona UTM – IPS, Web Filtering, AV, SSL Inspection

- IPS – Intrusion Prevention System:
 - Tworzenie IPS Profiles
 - Wykrywanie exploitów i blokowanie ataków
- Filtracja treści Web Filtering:
 - Blokowanie stron (blacklist, whitelist)
- SSL Deep Inspection – inspekcja ruchu HTTPS
- Kontrola aplikacji (Application Control):
 - Blokowanie ruchu P2P, VPN, TOR
 - Kategoryzacja aplikacji (YouTube, Social Media)
- Antywirus i Anti-Botnet:
 - Skanowanie AV w czasie rzeczywistym

- Blokowanie ruchu C2 (Command & Control)

5. Konfiguracja VPN IPSec Site-to-Site i SSL VPN

- IPSec Site-to-Site:
 - Konfiguracja tuneli IKEv1 vs IKEv2
 - NAT Traversal, Dead Peer Detection (DPD)
 - Troubleshooting (diagnose debug application ike)
- SSL VPN dla użytkowników zdalnych:
 - Konfiguracja SSL VPN Portal
 - Web Mode vs Tunnel Mode
 - Integracja z LDAP, RADIUS, 2FA

6. Routing i SD-WAN

- Routing statyczny vs dynamiczny:
 - OSPF, BGP, ECMP
 - Diagnostyka tras (get router info routing-table)
- SD-WAN – optymalizacja połączeń:
 - Tworzenie reguł SLA
 - Inteligentne przekierowanie ruchu
 - Diagnostyka SD-WAN (diagnose sys sdwan)

7. Zaawansowane mechanizmy bezpieczeństwa

- Role-Based Access Control (RBAC) – zarządzanie administratorami
- Integracja z Active Directory / LDAP
- Uwierzytelnianie wieloskładnikowe (2FA) – FortiToken

8. Monitorowanie i diagnostyka FortiGate

- Analiza logów systemowych (Log & Report)
- Syslog i SNMP Monitoring

- Packet Capture i analiza ruchu (Wireshark, FortiGate PCAP)
- Debugowanie ruchu sieciowego:
 - diagnose debug flow
 - diag sys session list
 - diag hardware sysinfo

9. Optymalizacja i zabezpieczenie systemu

- Hardening systemu FortiOS:
 - Minimalizacja powierzchni ataku
 - Blokowanie nieużywanych usług
 - Ograniczanie dostępu administracyjnego
- Zarządzanie aktualizacjami i podatnościami:
 - Patch management dla FortiOS
 - Automatyczne aktualizacje sygnatur IPS/AV

10. Warsztaty praktyczne i sesja Q&A

- Ćwiczenia CLI i GUI – rozwiązywanie rzeczywistych problemów
- Symulacja ataku i jego wykrywanie
- Konfiguracja tuneli VPN i troubleshooting
- Zarządzanie politykami firewall i kontrola ruchu