

Numer sprawy: 01/2026/cyberbezpieczeństwo

Panieńszczyzna dnia 08.01.2026r.

## Szczegółowy Opis Przedmiotu Zamówienia

Przeprowadzenie szkoleń z cyberbezpieczeństwa  
dla pracowników oraz dla administratora IT  
Urzędu Gminy w Jastkowie i Gminnego Ośrodka  
Pomocy Społecznej w Jastkowie

## Spis treści

1.	Zestawienie ilościowe.....	3
2.	Wymagania ogólne dla szkoleń. ....	3
3.	Opis przedmiotu zamówienia dla części nr 1.....	4
4.	Opis przedmiotu zamówienia dla części nr 2.....	6
5.	Opis przedmiotu zamówienia dla części nr 3.....	8
6.	Opis przedmiotu zamówienia dla części nr 4.....	9

## 1. Zestawienie ilościowe.

Lp.	Nazwa	Ilość	Część
1.	Zakup usług szkolenia administratora IT – szkolenie UTM	1 osoba	1
2.	Zakup usług szkolenia administratora IT – szkolenia autoryzowane CompTIA	1 osoba	2
3.	Zakup usług szkolenia administratora IT - szkolenie w zakresie audytu wewnętrznego	1 osoba	3
4.	Zakup usług szkolenia z cyberbezpieczeństwa dla pracowników	60 osób	4

Wykonawca może składać ofertę na poszczególne części zamówienia.

## 2. Wymagania ogólne dla szkoleń.

1. Jednostką czasową szkolenia jest 1 godzina szkoleniowa (1 godzina szkolenia = 45 minut).
2. Szkolenia będą trwały maksymalnie 8 godzin szkoleniowych w ciągu dnia.
3. Szkolenia będą odbywać się w dni robocze w godzinach 7.30 – 17.00.
4. Szkolenia będą prowadzone w języku polskim w formule stacjonarnej w siedzibie Wykonawcy lub Zamawiającego. Zamawiający nie dopuszcza prowadzenia szkoleń w trybie zdalnym w formule on-line.
5. Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego dziennego harmonogramu prac, dostarczonego przez Wykonawcę Zamawiającemu nie później niż 14 dni przed rozpoczęciem szkolenia.
6. Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego szczegółowego zakresu merytorycznego szkolenia dostarczonego przez Wykonawcę.
7. W przypadku szkoleń trwających do 3 godzin, przewiduje się jedną przerwę trwającą 15 minut. W przypadku szkoleń trwających powyżej 3 godzin, organizowane będą dwie przerwy trwające 15 minut każda. Dodatkowo, w przypadku szkoleń trwających 8 godzin zaplanowana jest przerwa trwająca 30 minut.
8. W ramach organizacji szkoleń Zamawiający zapewni rekrutację osób biorących udział w szkoleniach.
9. W ramach organizacji szkoleń Wykonawca zapewni:
  - a. Materiały szkoleniowe, obejmujące szczegółowy zakres szkolenia, harmonogram dzienny szkolenia oraz materiały merytoryczne (np. skrypty, podręczniki, zeszyty informacyjne, broszury) w formie papierowej lub elektronicznej, zawierające szczegółowe informacje, które będą omawiane podczas szkolenia. Ponadto w przypadku organizacji szkoleń w formule stacjonarnej (w siedzibie Zamawiającego), uczestnicy otrzymają materiały pisarskie, w tym zeszyty, długopisy, ołówki itp. Materiały szkoleniowe przekazywane są nieodpłatnie uczestnikom na własność. 2 egzemplarze materiałów szkoleniowych zostaną przekazane Zamawiającemu w celach archiwalnych.
  - b. W przypadku szkoleń stacjonarnych w siedzibie Zamawiającego oraz o ile wynika to z programu szkolenia Wykonawca zapewni sprzęt komputerowy dla każdego uczestnika

szkolenia umożliwiające przeprowadzenie szkolenia oraz wystarczającą liczbę własnych licencji na oprogramowanie komputerowe wykorzystywane przy realizacji szkoleń.

- c. Projektor multimedialny, tablice i inne artykuły niezbędne do prowadzenia szkoleń w przypadku prowadzenia szkoleń stacjonarnych w siedzibie Zamawiającego.
- d. Właściwe działania promocyjne i informacyjne dotyczące szkoleń, w tym właściwe oznakowanie sal szkoleniowych, jak również oznakowanie w odpowiedni sposób materiałów szkoleniowych przekazanych uczestnikom oraz Zamawiającemu w celach archiwalnych obowiązkowymi oznaczeniami Beneficjentów Funduszy Europejskich.
- e. Wydanie uczestnikom szkolenia imiennych zaświadczeń o ukończeniu danego szkolenia.
- f. Kadre trenerską posiadającą wiedzę i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkoleń.
- g. Prowadzenie dokumentacji szkoleń w jednaki sposób (dotyczy tylko i wyłącznie części nr 4 – szkolenia z cyberbezpieczeństwa dla pracowników). Na dokumentację szkolenia składają się:
  - Lista obecności uczestników szkolenia (dziennie, wypełniane oddzielnie każdego dnia szkolenia).
  - Lista odbioru zaświadczeń o ukończeniu szkolenia.
  - Potwierdzenie przez uczestników odbioru materiałów szkoleniowych.
  - Przeprowadzenie ankiet satysfakcji po każdym szkoleniu.
  - Sporządzony przez kadre trenerską dziennik zajęć, zawierający szczegółowe informacje na temat przebiegu oraz zakresu merytorycznego szkolenia, podpisany po zakończeniu szkolenia przez prowadzącego szkolenie.

### 3. Opis przedmiotu zamówienia dla części nr 1.

Przedmiotem zamówienia w tej części jest realizacja szkolenia w zakresie UTM dla administratora IT.

W ramach ramowego programu szkoleń Wykonawca powinien ująć minimum następujące zagadnienia:

1. W zakresie konfiguracji i użytkowania urządzenia UTM (Zamawiający posiada urządzenie firmy Fortigate) (min. 20 godzin szkoleniowych):
  - 1) Wstępna konfiguracja urządzenia UTM
    - Tryby pracy NAT/Transparent
    - Konfiguracja sieci i routingu
    - System Dashboard i moduły systemu
    - Administracja urządzeniem (WWW, CLI)
  - 2) Polityki zapory sieciowej
    - Koncepcja firewall w urządzeniach UTM
    - Tworzenie obiektów dla reguł firewall
    - Translacja adresów NAT i Virtual IP
  - 3) Optymalizacja ruchu sieciowego (kształtowanie pasma)
  - 4) Konfiguracja funkcji ochronnych (profile bezpieczeństwa)
    - Ochrona antywirusowa
    - Filtrowanie antyspamowe
    - System IPS / DoS Policy

- Kontrola ruchu WWW / blokowanie URL / DNS Filter
  - Kontrola aplikacji
  - Reputacja klienta
  - Data Leakage Prevention (DLP)
- 5) Inspekcja ruchu SSL
  - 6) Konfiguracja połączeń SSL VPN
  - 7) Bieżąca obsługa systemu
    - Tworzenie kopii zapasowej konfiguracji i jej odtwarzanie
    - Aktualizacja firmware
    - Administrowanie kontami użytkowników i profilami dostępu i) Logowanie i alerty
    - Omówienie sposobów logowania.
  - 8) Wirtualizacja w obrębie urządzenia – koncepcja wirtualnych domen (VDM)
    - Wykorzystanie trybów pracy NAT / Transparent
  - 9) Zaawansowana konfiguracja sieci i routingu
    - Tworzenie sieci VLAN
    - Routing dynamiczny
    - Pojęcie Policy Routingu
    - Load Balancing oraz redundancja łącz internetowych
  - 10) Uwierzytelnianie użytkowników
    - Integracja z usługami katalogowymi – FSSO
    - Tworzenie reguł firewall w oparciu o grupy użytkowników
    - Konta użytkowników gości
    - Dwuskładnikowa autoryzacja
    - Rozpoznawanie i uwierzytelnianie urządzeń
  - 11) Endpoint Control
    - Integracja z aplikacją zarządzania urządzeniem końcowym
  - 12) Wirtualne sieci prywatne (VPN)
    - IPSec VPN site-to-site client-to-site
    - Rozwiązywanie problemów z połączeniami VPN
  - 13) Diagnostyka i rozwiązywanie problemów
  - 14) Konfiguracja urządzeń do pracy w klastrze HA
    - Tryby pracy klastra
    - Topologia połączeń i konfiguracja urządzeń

#### Dodatkowe wymagania:

1. W ramach usługi zostanie przeszkolona 1 osoba.
2. Szkolenie powinno trwać łącznie minimum 20 godzin szkoleniowych dla jednej osoby.
3. Usługi szkoleniowe dotyczące UTM muszą być wykonane przez osobę lub osoby posiadające certyfikat producenta sprzętu lub oprogramowania w zakresie odpowiadającym przedmiotowi szkolenia i wiedzę z zakresu instalacji, konfigurowania oraz zarządzania sprzętem lub oprogramowaniem.
4. Szkolenia mogą trwać nie dłużej niż do 31 maja 2026 r.
5. Uczestnik po zakończeniu szkolenia otrzyma certyfikat lub zaświadczenie lub inny dokument potwierdzający uczestnictwo w szkoleniu.

## 4. Opis przedmiotu zamówienia dla części nr 2.

Przedmiotem zamówienia w tej części jest realizacja autoryzowanych szkoleń CompTIA dla administratora IT.

W ramach ramowego programu szkoleń Wykonawca powinien ująć minimum następujące zagadnienia:

1. W zakresie certyfikacji CompTIA Network+ (min. 35 godzin szkoleniowych):
  - 1) Architektura sieciowa i model referencyjny OSI.
  - 2) Okablowanie sieci Ethernet.
  - 3) Przełączanie w sieciach Ethernetowych.
  - 4) Rozwiązywanie problemów sieci Ethernet.
  - 5) Protokół IPv4.
  - 6) Wsparcie dla sieci IPv4 i IPv6.
  - 7) Konfigurowanie i rozwiązywanie problemów z routerami.
  - 8) Topologie i typy sieci.
  - 9) Protokoły warstwy transportowej.
  - 10) Usługi sieciowe.
  - 11) Aplikacje sieciowe.
  - 12) Dostępność sieci.
  - 13) Bezpieczeństwo sieci.
  - 14) Rozwiązywanie problemów w zabezpieczonych sieciach.
  - 15) Rozwiązywanie problemów w sieciach bezprzewodowych.
  - 16) Łącza WAN i metody zdalnego dostępu.
  - 17) Koncepcje bezpieczeństwa organizacyjnego i fizycznego.
  - 18) Disaster Recovery i High Availability.
  - 19) Techniki zabezpieczania sieci.
  - 20) Architektura chmury i centrum danych.
2. W zakresie certyfikacji CompTIA Security+ (min. 35 godzin szkoleniowych):
  - 1) Definicja bezpieczeństwa informacji;
  - 2) Cele bezpieczeństwa: poufność, integralność, dostępność (CIA triad);
  - 3) Cykl życia zarządzania ryzykiem;
  - 4) Zasady ochrony danych;
  - 5) Typy ryzyka: ryzyko operacyjne, strategiczne, techniczne;
  - 6) Identyfikacja, ocena i zarządzanie ryzykiem;
  - 7) Działania w odpowiedzi na ryzyko: unikanie, łagodzenie, akceptacja, transfer;
  - 8) Ataki sieciowe (np. DDoS, sniffing);
  - 9) Malware (wirusy, trojany, ransomware);
  - 10) Phishing i social engineering;
  - 11) Aplikacje i exploity;
  - 12) Inne zagrożenia (e.g. insider threats);
  - 13) Zasady ochrony przed atakami z sieci;

- 14) Oprogramowanie ochrony przed malwarem i atakami;
  - 15) Firewalle, IDS/IPS (Intrusion Detection/Prevention Systems);
  - 16) VPN i zdalny dostęp;
  - 17) Ochrona przed atakami (np. ACL, NAT);
  - 18) Rodzaje kryptografii: symetryczna, asymetryczna, hashowanie;
  - 19) Zastosowania SSL/TLS, HTTPS;
  - 20) Certyfikaty cyfrowe, PKI (Public Key Infrastructure);
  - 21) Algorytmy kryptograficzne i ich zastosowanie;
  - 22) Modele chmurowe: IaaS, PaaS, SaaS;
  - 23) Ryzyka i bezpieczeństwo chmury;
  - 24) Zasady ochrony danych w chmurze;
  - 25) Metody uwierzytelniania: hasła, uwierzytelnianie wieloskładnikowe (MFA), biometryczne;
  - 26) Systemy Single Sign-On (SSO);
  - 27) Zasady zarządzania uprawnieniami;
  - 28) Zabezpieczanie kont użytkowników;
  - 29) Kontrola dostępu na podstawie ról (RBAC);
  - 30) Implementacja polityk dostępu;
  - 31) Metody szyfrowania danych: w spoczynku, w trakcie przesyłania;
  - 32) Zarządzanie kluczami szyfrowania;
  - 33) Zabezpieczanie urządzeń mobilnych i nośników danych;
  - 34) Planowanie backupów;
  - 35) Procesy odzyskiwania danych po awarii (Disaster Recovery, Business Continuity);
  - 36) Zasady ochrony danych w systemach rozproszonych;
  - 37) Cykl życia incydentu bezpieczeństwa;
  - 38) Zasady tworzenia planu odpowiedzi na incydenty;
  - 39) Zbieranie dowodów i analiza incydentów;
  - 40) Zbieranie i analiza logów;
  - 41) Testowanie odporności na ataki: Red Team, Blue Team;
  - 42) Użycie SIEM (Security Information and Event Management);
  - 43) Monitorowanie ruchu sieciowego;
  - 44) Analiza zagrożeń i podatności;
  - 45) Dokumentacja wyników audytów;
  - 46) Sporządzanie raportów bezpieczeństwa.
3. W zakresie certyfikacji CompTIA Serwer+ (min. 35 godzin szkoleniowych):
- 1) Instalacja sprzętu fizycznego: montaż w szafach, okablowanie, zarządzanie zasilaniem i chłodzeniem.
  - 2) Wdrażanie i zarządzanie pamięcią masową: poziomy RAID, pamięć współdzielona i planowanie pojemności.
  - 3) Konserwacja sprzętu: zarządzanie poza pasmem, aktualizacje oprogramowania układowego i komponenty z możliwością wymiany podczas pracy.
  - 4) Instalacja systemów operacyjnych serwerów: typy partycji, systemy plików i metody instalacji.
  - 5) Konfiguracja usług sieciowych: adresowanie IP, DNS, DHCP i sieci VLAN.

- 6) Zarządzanie funkcjami serwera: role, monitorowanie, migracja danych i wskaźniki wydajności.
- 7) Wysoka dostępność: klastrowanie, równoważenie obciążenia i procesy przełączania awaryjnego.
- 8) Wirtualizacja: host a gość, alokacja zasobów i modele chmury.
- 9) Podstawy skryptów: pętle, zmienne i typowe zadania serwerowe.
- 10) Zarządzanie zasobami: dokumentacja, zarządzanie cyklem życia i bezpieczne przechowywanie.
- 11) Bezpieczeństwo danych: szyfrowanie, zasady przechowywania i zarządzanie cyklem życia.
- 12) Bezpieczeństwo fizyczne: kontrola dostępu, kontrola środowiska i systemy biometryczne.
- 13) Zarządzanie tożsamością i dostępem: konta użytkowników, MFA i uprawnienia.
- 14) Strategie ograniczania ryzyka: zapobieganie złośliwemu oprogramowaniu, DLP i SIEM.
- 15) Zabezpieczanie serwerów: aktualizacje systemu operacyjnego, wyłączanie nieużywanych usług i bezpieczeństwo hosta.
- 16) Wycofywanie z eksploatacji: niszczenie nośników, recykling i zarządzanie zasobami.
- 17) Rozwiązywanie problemów sprzętowych: problemy z zasilaniem, awarie pamięci masowej i problemy z łącznością.
- 18) Rozwiązywanie problemów związanych z oprogramowaniem: błędy systemu operacyjnego, problemy z aplikacjami i awarie poprawek.
- 19) Rozwiązywanie problemów związanych z siecią: opóźnienia, nieprawidłowe konfiguracje i naruszenia bezpieczeństwa.
- 20) Odzyskiwanie danych po awarii: strategie tworzenia kopii zapasowych, testowanie odzyskiwania danych i weryfikacja przełączania awaryjnego.

#### Dodatkowe wymagania:

1. W ramach usługi zostanie przeszkolona 1 osoba.
2. Szkolenie powinno trwać łącznie minimum 105 godzin szkoleniowych dla jednej osoby.
3. Usługi szkoleniowe dotyczące certyfikacji CompTIA muszą być przeprowadzone w autoryzowanym ośrodku CompTIA przez autoryzowanego trenera CompTIA.
4. Szkolenia mogą trwać nie dłużej niż do 31 maja 2026 r.
5. Uczestnik po zakończeniu szkolenia otrzyma certyfikat lub zaświadczenie lub inny dokument potwierdzający uczestnictwo w szkoleniu.

## 5. Opis przedmiotu zamówienia dla części nr 3.

Przedmiotem zamówienia w tej części jest realizacja szkoleń w zakresie audytora wewnętrznego Systemu Zarządzania Bezpieczeństwem Informacji ISO 27001 dla administratora IT.

W ramach ramowego programu szkoleń Wykonawca powinien ująć minimum następujące zagadnienia:

1. W zakresie audytora wewnętrznego Systemu Zarządzania Bezpieczeństwem Informacji ISO 27001 (min. 15 godzin szkoleniowych):
  - 1) Pojęcie bezpieczeństwa informacji.
  - 2) Norma ISO 27001 jako model budowy Systemu Zarządzania Bezpieczeństwem Informacji.
  - 3) Wymagania normy ISO 27001



- 4) Wymagania systemowe - PDCA, szacowanie i zarządzanie ryzykiem.
- 5) Audyty systemu.
- 6) Przeglądy systemu.
- 7) Doskonalenie systemu.
- 8) Planowanie audytu.
- 9) Prowadzenie badań audytowych.
- 10) Identyfikacja niezgodności.
- 11) Dokumentowanie wyników audytu.
- 12) Udział w działaniach doskonalących.

Dodatkowe wymagania:

1. W ramach usługi zostanie przeszkolona 1 osoba.
2. Szkolenie powinno trwać łącznie minimum 15 godzin szkoleniowych dla jednej osoby.
3. Szkolenia mogą trwać nie dłużej niż do 31 maja 2026 r.
4. Uczestnik po zakończeniu szkolenia otrzyma certyfikat lub zaświadczenie lub inny dokument potwierdzający uczestnictwo w szkoleniu.

## 6. Opis przedmiotu zamówienia dla części nr 4.

Przedmiotem zamówienia w tej części jest realizacja szkoleń z cyberbezpieczeństwa dla pracowników Urzędu Gminy w Jastkowie oraz Gminnego Ośrodka Pomocy Społecznej w Jastkowie.

W ramach ramowego programu szkoleń Zamawiający zaleca ująć następujące zagadnienia:

1. Główne założenia i wymagania prawne cyberbezpieczeństwa w pracy urzędnika.
2. Polityka bezpieczeństwa w organizacji.
3. Definicja incydentu bezpieczeństwa i zasady postępowania z incydemem.
4. Rodzaje ataków: ataki socjotechniczne, ataki komputerowe, ataki przez sieci bezprzewodowe, ataki przez pocztę e-mail (fałszywe e-maile), ataki przez strony WWW, ataki przez telefon, phishing, spoofing, spam.
5. Bezpieczeństwo fizyczne - urządzenia, dokumenty, „czyste biurko”.
6. Zabezpieczenie informatycznych nośników danych – pendrivy i pamięci zewnętrzne.
7. Zdalny dostęp do zasobów jednostki i korzystanie z urządzeń prywatnych przez pracowników oraz związane z tym potencjalne zagrożenia.
8. Przechowywanie danych w chmurze i korzystanie z zewnętrznych dostawców usług informatycznych.
9. Prawidłowe korzystanie z oprogramowania antywirusowego.
10. Zasady aktualizacji programów i aplikacji.
11. Szyfrowanie dokumentów i poczty elektronicznej.
12. Polityka haseł, zarządzanie dostępem i tożsamością.

Dodatkowe wymagania:

1. W ramach usługi zostanie przeszkolone 60 osób w 5 grupach maksimum 15-osobowych.
2. Szkolenie powinno trwać minimum 6 godzin szkoleniowych dla 1 grupy szkoleniowej.
3. Szkolenia mogą trwać nie dłużej niż do 31 maja 2026 r.