Załącznik nr 4

do Zapytania ofertowego

|  |  |
| --- | --- |
| BZP.271.4.8.2026 | Krasnystaw, dnia 16.02.2026 r. |
| Opis Przedmiotu Zamówienia  Zakup usług przeprowadzenia szkoleń dla pracowników Urzędu Miasta Krasnystaw i jednostek organizacyjnych Miasta Krasnystaw związanych z realizacją projektu „Cyberbezpieczny Samorząd” | |

Spis treści

[1. Zestawienie ilościowe. 3](#_Toc209689044)

[2. Wymagania ogólne dla szkoleń. 3](#_Toc209689045)

[3. Zakup usług szkolenia administratora IT. 4](#_Toc209689046)

[4. Zakup usług szkolenia pracowników z cyberbezpieczeństwa. 7](#_Toc209689047)

# Zestawienie ilościowe.

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa | Ilość |
| 1. | Zakup usług szkolenia administratora IT | 1 |
| 2. | Zakup usług szkolenia pracowników z cyberbezpieczeństwa | 100 |

# 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 – 15.30.
4. Szkolenia będą prowadzone w języku polskim w formule stacjonarnej w siedzibie Zamawiającego. Zamawiający dopuszcza prowadzenie szkoleń dla administratora w trybie zdalnym w formule on-line.
5. Szkolenia prowadzone będą na podstawie zaakceptowanego prze Zamawiającego dziennego harmonogramu prac, dostarczonego przez Wykonawcę Zamawiającemu nie później niż 3 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. Wykonawca jest zobowiązany do przeprowadzenia szkolenia uzupełniającego dla osób, które nie ze względów przypadków losowych nie będą mogły uczestniczyć w szkoleniu   
   w wyznaczonych terminach.
9. W ramach organizacji szkoleń Wykonawca zapewni:
   1. 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.
   2. W przypadku szkoleń prowadzonych w trybie zdalnym w formule on-line Wykonawca jest zobowiązany dostarczyć narzędzia do komunikacji zdalnej, które umożliwią dwustronne przesyłanie przez sieć Internet obrazu i dźwięku między prowadzącym szkolenie   
      a uczestnikami szkolenia. Narzędzie musi umożliwiać zadawanie pytań także w formie pisemnej bezpośrednio na czacie w trakcie trwania sesji szkoleniowej. W przypadku szkolenia prowadzonego w trybie zdalnym w formule on-line Zamawiający zastrzega możliwość nagrania szkolenia, a Wykonawca musi zapewnić wyrażenie na to zgody osoby prowadzącej szkolenie.
   3. W przypadku szkoleń stacjonarnych (w siedzibie Zamawiającego) oraz o ile wynika to z programu szkolenia Wykonawca zapewni sprzęt komputerowy dla każdego uczestnika szkolenia umożliwiający przeprowadzenie szkolenia oraz wystarczającą liczbę własnych licencji na oprogramowanie komputerowe wykorzystywane przy realizacji szkoleń.
   4. Projektor multimedialny, tablice i inne artykuły niezbędne do prowadzenia szkoleń w przypadku prowadzenia szkoleń stacjonarnych (w siedzibie Zamawiającego).
   5. 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.
   6. Wydanie uczestnikom szkolenia zaświadczeń o ukończeniu danego szkolenia.
   7. Kadrę trenerską posiadającą wiedzę i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkoleń.
   8. Prowadzenie dokumentacji wszystkich szkoleń w jednakowy sposób. Na dokumentację szkolenia składają się:
      * Lista obecności uczestników szkolenia (dzienne, 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 kadrę trenerską dziennik zajęć, zawierający szczegółowe informacje na temat przebiegu oraz zakresu merytorycznego szkolenia, podpisany po zakończeniu szkolenia przez prowadzącego szkolenie.

# Zakup usług szkolenia administratora IT.

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

1. Rejestracja Urządzeń w Systemie: Proces dodawania nowych urządzeń do systemu zarządzania. Konfiguracja parametrów urządzeń oraz weryfikacja poprawności rejestracji; Automatyczne wykrywanie urządzeń i integracja z istniejącymi zasobami.
2. Zarządzanie Licencjami i Subskrypcjami: Przegląd dostępnych licencji i subskrypcji. o Procedury aktywacji i odnawiania licencji; Monitorowanie zużycia licencji oraz optymalizacja kosztów.
3. Procedura Aktualizacji Oprogramowania: Przeprowadzanie aktualizacji firmware'u   
   i oprogramowania urządzeń. Zasady bezpiecznego przeprowadzania aktualizacji (kopie zapasowe, testowanie); Automatyzacja procesu aktualizacji i harmonogramowanie.
4. Zmiana Danych Dostępowych (Autoryzacja) do Urządzeń: Procedury zmiany haseł i danych autoryzacyjnych; Implementacja polityk zmiany haseł i zarządzania dostępem. Audytowanie   
   i zabezpieczanie danych dostępowych.
5. Konfiguracja Metod Dostępu do Urządzeń: Implementacja i konfiguracja bezpiecznego dostępu do urządzeń; Zarządzanie certyfikatami SSL/TLS.
6. Wdrożenie Dwuetapowej Autoryzacji (2FA): Implementacja 2FA dla zwiększenia bezpieczeństwa dostępu; Konfiguracja aplikacji autoryzujących i tokenów sprzętowych.
7. Ustawienie Podstawowych Łącz Internetowych: Konfiguracja głównych połączeń internetowych; Monitorowanie i optymalizacja wydajności łączy; Konfiguracja Łącz Zapasowych i Redundancji (WAN): Implementacja zapasowych łączy internetowych; Konfiguracja mechanizmów przełączania awaryjnego i load balancingu.
8. Segmentacja Sieci LAN: Konfiguracja Interfejsów Sieciowych: Ustawienia interfejsów fizycznych   
   i logicznych; Optymalizacja parametrów interfejsów dla różnych zastosowań.
9. Konfiguracja VLAN i Polityk Dostępu do Podsieci/VLAN: Tworzenie i zarządzanie VLANami.; Implementacja polityk bezpieczeństwa dla poszczególnych VLANów.
10. Zarządzanie Siecią i Polityki Bezpieczeństwa: Uruchomienie Serwerów DHCP: Konfiguracja Serwerów DHCP na Poszczególnych Podsieciach/VLAN: Ustawienia serwerów DHCP dla dynamicznego przydzielania adresów IP; Zarządzanie pulami adresów i rezerwacjami; Konfiguracja Routingu i Agregacji Portów: Ustawienia Routingu Statycznego i Dynamicznego: Konfiguracja tras statycznych i protokołów routingu dynamicznego (OSPF, BGP); Optymalizacja trasowania i zarządzanie tablicami routingu. Konfiguracja Agregacji Portów dla Zwiększenia Przepustowości: Implementacja agregacji portów (LACP); Balansowanie obciążenia i redundancja portów.
11. Polityki Bezpieczeństwa. Filtrowanie i Blokowanie Treści oraz Aplikacji Internetowych: Konfiguracja filtrów treści i aplikacji; Zarządzanie czarnymi i białymi listami.
12. Konfiguracja Antywirusa, Filtrów DNS, IPS i DLP: Implementacja zabezpieczeń antywirusowych   
    i systemów wykrywania intruzji (IPS); Konfiguracja filtrów DNS i polityk zapobiegania wyciekom danych (DLP).
13. Integracja i Zarządzanie Systemem. Integracja z Domeną: Konfiguracja Urządzeń do Współpracy   
    z Domena: Procedury integracji z domeną Active Directory; Zarządzanie kontami i politykami bezpieczeństwa domeny.
14. Konfiguracja SNMP. Ustawienia SNMP do Monitorowania Sieci: Konfiguracja protokołu SNMP dla monitorowania i zarządzania urządzeniami sieciowymi; Implementacja pułapek SNMP i zbieranie danych z urządzeń.
15. Logowanie, Kopie Zapasowe i VPN. Konfiguracja Procesu Logowania: Konfiguracja Zawartości Logów i Okresu Przechowywania: Definiowanie typów logów, które mają być przechowywane; Ustalanie okresów retencji logów i zarządzanie przestrzenią dyskową.
16. Wykonanie Kopii Zapasowej Ustawień Urządzeń: Procedury Tworzenia Kopii Zapasowych   
    i Przywracania Ustawień: Automatyzacja tworzenia kopii zapasowych ustawień urządzeń; Procedury przywracania ustawień z kopii zapasowych.
17. Konfiguracja Tuneli VPN IPsec / SSL. Konfiguracja Tuneli VPN Typu IPsec i SSL: Tworzenie   
    i zarządzanie tunelami VPN dla bezpiecznej komunikacji; Konfiguracja polityk bezpieczeństwa VPN i zarządzanie certyfikatami.

Dodatkowe wymagania:

1. W ramach usługi zostanie przeszkolona 1 osoba.
2. Szkolenie powinno trwać minimum 120 godzin szkoleniowych dla jednej osoby.

# Zakup usług szkolenia pracowników z cyberbezpieczeństwa.

W ramach ramowego programu szkoleń Wykonawca powinien ująć minimum 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 incydentem.
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 100 osób w maksymalnie 4 grupach maksimum   
   25-osobowych.
2. Szkolenie powinno trwać minimum 3 godzin szkoleniowych dla 1 grupy szkoleniowej.