Załącznik nr 4

do Zapytania ofertowego

nr PG.271.4.2022

Szczegółowy Opis Przedmiotu Zamówienia

1. **Przedmiot zamówienia:**

   „Przeprowadzenie szkolenia dla urzędników w zakresie cyberbezpieczeństwa w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina" o numerze POPC.05.01.00-00-0001/21-00";

2. **Zestawienie ilościowe**

L.P.	Nazwa	Ilość
1.	Przeprowadzenie szkoleń w zakresie cyberbezpieczeństwa dla urzędników	• 2 grupy szkoleniowe po około 35 uczestników; • czas trwania szkolenia dla jednej grupy szkoleniowej: minimum 3 godziny.

3. **<u>Wymagania ogólne dla szkoleń:</u>**

   a) Szkolenie z zakresu cyberbezpieczeństwa w Urzędzie Miasta Hajnówka zostanie przeprowadzone w formie zdalnej.

   b) Jednostką czasową szkolenia jest 1 godzina zegarowa (60 minut).

   c) Szkolenia będą trwały minimum 3 godziny dla jednej grupy szkoleniowej (2 grupy * 3 godziny = minimum 6 godzin szkoleniowych łącznie).

   d) Szkolenia będą odbywać się w dni robocze w godzinach 7.30 – 15.30.

   e) Szkolenia będą prowadzone w języku polskim.

   f) Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego harmonogramu zawierającego zakres merytoryczny, dostarczonego przez Wykonawcę Zamawiającemu nie później niż 3 dni przed rozpoczęciem szkolenia.

   g) 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.

h) W ramach organizacji szkoleń Wykonawca zapewni:
   - Materiały szkoleniowe, obejmujące szczegółowy zakres szkolenia oraz harmonogram dzienny szkolenia w formie elektronicznej, zawierające szczegółowe informacje, które będą omawiane podczas szkolenia. Materiały szkoleniowe przekazywane są nieodpłatnie Uczestnikom na własność. Dwa egzemplarze materiałów szkoleniowych zostaną przekazane Zamawiającemu w celach archiwalnych;
   - Dostęp do platformy szkoleniowej lub platformy wideokonferencji umożliwiającej przeprowadzenie szkolenia;
   - Wydanie Uczestnikom szkolenia zaświadczeń o ukończeniu danego szkolenia;
   - Kadrę trenerską posiadającą wiedzę i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkoleń.
   - Prowadzenie dokumentacji wszystkich szkoleń w jednakowy sposób. Na dokumentację szkolenia składają się: Lista obecności Uczestników szkolenia, Lista wydanych zaświadczeń o ukończeniu szkolenia, Sporządzony przez kadrę trenerską protokół z każdego z dwóch szkoleń, zawierający szczegółowe informacje na temat przebiegu oraz zakresu merytorycznego szkolenia, podpisany po zakończeniu szkolenia przez prowadzącego szkolenie.

4. Ramowy zakres szkolenia:

W programie szkolenia muszą być ujęte poniższe zagadnienia:

a) Prawne aspekty bezpieczeństwa informacji i cyberbezpieczeństwa.
b) Obowiązki jednostek publicznych w obszarze bezpieczeństwa informacji.
c) Spam jako sposób na ataki.
d) Dezinformacja i fake newsy jako skuteczna broń na froncie wojny informacyjnej.
e) Kradzieże i wyłudzenia informacji – przykłady z życia urzędów.
f) Cyberbezpieczeństwo w pracy zdalnej – dobre praktyki/wskazówki.
g) Proste i skuteczne metody codziennej ochrony informacji:
   - Pendrive, dysk przenośny - użytkowanie, źródło niebezpieczeństwa.

- Przekazywanie haseł dostępowych współpracownikom.
- Jak tworzyć silne hasła i jak zapamiętać?
- Phishing, czyli jak odróżnić fałszywą korespondencję e-mail przychodzącą do urzędu?
- Zachowanie poufności przesyłanych dokumentów.
- Metadane w dokumentach opublikowanych w BIP. Czy są cenne dla przestępców?
- Ataki socjotechniczne - czyli niewinne „wyłudzanie” danych.