Numer sprawy: **ROSS.271.16.2022**

24.03.2022

Załącznik nr 1 do
Zapytania ofertowego znak **ROSS.271.16.2022**

Szczegółowy Opis Przedmiotu Zamówienia

Spis treści

1. Zestawienie ilościowe.

Przeprowadzeniu diagnozy cyberbezpieczeństwa oraz szkoleń z zakresu cyberbezpieczeństwa

Lp.	Nazwa	Ilość
1.	Przeprowadzenie szkolenia dla urzędników w zakresie cyberbezpieczeństwa	62 osoby
2.	Przeprowadzenie diagnozy cyberbezpieczeństwa	1 szt.

2. Przedmiot zamówienia

2.1. Przeprowadzenie szkolenia w zakresie cyberbezpieczeństwa.

Wymagania ogólne dla szkoleń:

1. Jednostką czasową szkolenia jest 1 godzina szkoleniowa (1 godzina szkolenia = 45 minut).
2. Szkolenia będą trwały maksymalnie 5 godzin szkoleniowych w ciągu dnia.
3. Szkolenia będą odbywać się w dni robocze w godzinach 7.30 – 14.30.
4. Szkolenia będą prowadzone w języku polskim.
5. Szkolenia prowadzone będą na podstawie zaakceptowanego prze Zamawiającego dziennego harmonogramu prac, dostarczonego przez Wykonawcę Zamawiającemu nie później niż 7 dni przed rozpoczęciem szkolenia. Zamawiający zastrzega, że szkolenia nie powinny odbywać się częściej niż jedna grupa szkoleniowa w tygodniu.
6. Szkolenia prowadzone będą na podstawie zaakceptowanego prze Zamawiającego szczegółowego zakresu merytorycznego szkolenia dostarczonego przez Wykonawcę.
7. W przypadku szkoleń trwających 5 godzin przewiduje się jedną przerwę trwającą 30 minut lub 2 przerwy po 15 minut, (przerw nie wlicza się do czasu szkolenia).
8. W ramach organizacji szkoleń Zamawiający zapewni rekrutację osób biorących udział w szkoleniach.
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, zawierające szczegółowe informacje, które będą omawiane podczas szkolenia. Ponadto, 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) Dostęp do sieci Internet.
   3) Warunki pracy uczestników i Wykonawcy w trakcie trwania szkolenia zgodne przepisami bezpieczeństwa i higieny pracy.

4) Wystarczającą liczbę własnych licencji na oprogramowanie komputerowe wykorzystywane przy realizacji szkoleń oraz sprzęt komputerowy dla każdego Uczestnika umożliwiający przeprowadzenie szkolenia.
5) Projektor multimedialny, tablice i inne artykuły niezbędne do prowadzenia szkoleń.
6) 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.
7) Wydanie Uczestnikom szkolenia zaświadczeń o ukończeniu danego szkolenia.
8) Kadrę trenerską posiadającą wiedzę i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkoleń.
9) Prowadzenie dokumentacji wszystkich szkoleń w jednakowy sposób. Na dokumentację szkolenia składają się:
   a) Lista obecności Uczestników szkolenia (dzienne, wypełniane oddzielnie każdego dnia szkolenia).
   b) Lista odbioru zaświadczeń o ukończeniu szkolenia.
   c) Potwierdzenie przez Uczestników odbioru materiałów szkoleniowych.
   d) Przeprowadzenie ankiet satysfakcji po każdym szkoleniu.
   e) Sporządzony przez kadrę trenerską dziennik zajęć, zawierający szczegółowe informacje na temat przebiegu oraz zakresu merytorycznego szkolenia, podpisany po zakończeniu szkolenia przez prowadzącego szkolenie.

<u>Ramowy zakres szkolenia:</u>

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. Prawidłowe korzystanie z oprogramowania antywirusowego.
7. Zasady aktualizacji programów i aplikacji.
8. Szyfrowanie dokumentów i poczty elektronicznej.
9. Polityka haseł, zarządzanie dostępem i tożsamością.

<u>Dodatkowe wymagania:</u>

1. W ramach usługi zostaną przeszkolone 62 osoby w grupach minimum 10-osobowych. Zamawiający zastrzega możliwość skierowania do grupy większej ilości osób.
2. Szkolenie powinno odbywać się na terenie Gminy Nowa Słupia.
3. Szkolenie musi być prowadzone w języku polskim.
4. Szkolenie powinno trwać 5 godzin szkoleniowych dla 1 grupy szkoleniowej.

2.2. Przeprowadzenie diagnozy cyberbezpieczeństwa.

1. Wykonawca przeprowadzi diagnozę cyberbezpieczeństwa jednostki samorządu terytorialnego – Urzędu Miasta i Gminy w Nowej Słupi.
2. Diagnoza musi być przeprowadzona w zakresie określonym w „Formularzu informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa" stanowiącym załącznik nr 8 do Regulaminu Konkursu Grantowego Cyfrowa Gmina (załączony do Zapytania ofertowego jako Załącznik nr 4).
3. Diagnoza musi być przeprowadzona przez osobę posiadającą certyfikat uprawniający do przeprowadzenia audytu, o którym mowa w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.
4. Wykonawca przekaże wynik przeprowadzonej diagnozy w postaci pliku wypełnionego arkusza kalkulacyjnego formularza, o którym mowa w pkt. 2, podpisanego podpisem cyfrowym (weryfikowanym certyfikatem kwalifikowanym lub przy wykorzystaniu profilu zaufanego) przez osobę posiadającą uprawnienia, o których mowa w pkt. 3.
5. Jednostki samorządu terytorialnego biorące udział w projekcie „Cyfrowa Gmina" są zobowiązane do przeprowadzenia diagnozy cyberbezpieczeństwa będącej przedmiotem niniejszego zamówienia. Niezwłocznie po jej przeprowadzeniu, jej wyniki mają być przekazane przez Zamawiającego do Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego (NASK) za pośrednictwem platformy ePUAP. Dane z diagnozy przekazane przez JST do NASK posłużą do opracowania raportu na temat stanu bezpieczeństwa systemów jednostek samorządowych. Wykonawca jest zobowiązany mieć na uwadze powyższy cel przeprowadzenia diagnozy i jej przeznaczenie.