Jastrząb, dnia 07.04.2022r.

Załącznik nr 1

Szczegółowy Opis Przedmiotu Zamówienia

Przeprowadzenia diagnozy cyberbezpieczeństwa oraz szkoleń w zakresie cyberbezpieczeństwa

Lp.	Nazwa	Ilość
1.	Przeprowadzenie szkolenia dla urzędników w zakresie cyberbezpieczeństwa	28 osób
2.	Przeprowadzenie diagnozy cyberbezpieczeństwa	1 szt.

Przeprowadzenie szkoleń 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 – 15.30.
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 14 dni przed rozpoczęciem szkolenia.
6. Szkolenia prowadzone będą na podstawie zaakceptowanego prze 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.
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. Materiały szkoleniowe przekazywane są nieodpłatnie Uczestnikom na własność. 2 egzemplarze materiałów szkoleniowych zostaną przekazane Zamawiającemu w celach archiwalnych.
   2) Warunki pracy uczestników i Wykonawcy w trakcie trwania szkolenia zgodne przepisami bezpieczeństwa i higieny pracy.
   3) Właściwe działania promocyjne i informacyjne dotyczące szkoleń, w tym oznakowanie w odpowiedni sposób materiałów szkoleniowych przekazanych Uczestnikom oraz Zamawiającemu w celach archiwalnych obowiązkowymi oznaczeniami Beneficjentów Funduszy Europejskich.
   4) Wydanie Uczestnikom szkolenia zaświadczeń o ukończeniu danego szkolenia.
   5) Kadrę trenerską posiadającą wiedzę i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkoleń. **Wykonawca musi udokumentować min. 3-letnie doświadczenie kadry trenerskiej.**
   6) 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.

Ramowy zakres szkolenia:

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. Szyfrowanie dokumentów i poczty elektronicznej.
11. Polityka haseł, zarządzanie dostępem i tożsamością.

Dodatkowe wymagania:

1. W ramach usługi zostanie przeszkolonych 28 osób w grupach maksimum 7-osobowych.
2. Szkolenie powinno odbywać się na terenie Gminy Jastrząb.
3. Szkolenie musi być prowadzone w języku polskim.
4. Szkolenie powinno trwać minimum 5 godzin szkoleniowych dla 1 grupy szkoleniowej.

Przeprowadzenie diagnozy cyberbezpieczeństwa.

1. Wykonawca przeprowadzi diagnozę cyberbezpieczeństwa jednostki samorządu terytorialnego – Urzędu Gminy Jastrząb.
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.