Załącznik nr 1 do zapytania ofertowego

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

na wykonanie zadania: „Przeprowadzenie diagnozy cyberbezpieczeństwa oraz przeprowadzenie stacjonarnego szkolenia w zakresie cyfrowego bezpieczeństwa informacji w Urzędzie Gminy Lipce Reymontowskie" 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

CZĘŚĆ I
PRZEPROWADZENIE DIAGNOZY CYBERBEZPIECZEŃSTWA

1. W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany będzie do dokonania oceny zgodności funkcjonujących zasad i procedur dotyczących zarządzania bezpieczeństwem informacji w Urzędzie Gminy Lipce Reymontowskie, w tym:
   1) ocenę zgodności z ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa,
   2) ocenę bezpieczeństwa systemów informatycznych.

2. Diagnoza cyberbezpieczeństwa w Urzędzie Gminy Lipce Reymontowskie musi zostać przeprowadzona zgodnie z Ustawą z dnia 5 lipca 2018 r. ***o krajowym systemie cyberbezpieczeństwa*** (Dz.U. z 2018 r. poz. 1560 z późn. zm.)

3. Diagnoza cyberbezpieczeństwa musi zostać przeprowadzona zgodnie z formularzem zamieszczonym w dokumentacji konkursowej projektu Cyfrowa Gmina dostępnym na stronach Centrum Projektów Polska Cyfrowa [https://www.gov.pl/web/cppc/cyfrowa-gmina] - ***Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa - załącznik nr 8.***

4. Diagnoza cyberbezpieczeństwa musi zostać przeprowadzony przez osobę posiadającą uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Wykaz certyfikatów wskazanych w ww. rozporządzeniu:
   1) Certified Internal Auditor (CIA),
   2) Certified Information System Auditor (CISA),
   3) Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób,
   4) Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób,
   5) Certified Information Security Manager (CISM),
   6) Certified in Risk and Information Systems Control (CRISC),
   7) Certified in the Governance of Enterprise IT (CGEIT),
   8) Certified Information Systems Security Professional (CISSP),
   9) Systems Security Certified Practitioner (SSCP),
   10) CertifiedReliability Professional,
   11) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

5. Diagnoza cyberbezpieczeństwa musi być przeprowadzona w siedzibie Zamawiającego osobiście przez Wykonawcę, nie dopuszcza się formy zdalnej przeprowadzenia diagnozy.

6. Zamawiający nie zezwala Wykonawcy na powierzenie prac związanych z wykonaniem diagnozy cyberbezpieczeństwa osobom trzecim.

7. Wykonawca omówi wyniki przeprowadzonej diagnozy cyberbezpieczeństwa w siedzibie Zamawiającego.

8. Diagnozę cyberbezpieczeństwa należy dostarczyć w wersji elektronicznej oraz w wersji papierowej.

CZĘŚĆ II
PRZEPROWADZENIE SZKOLENIA Z ZAKRESU CYFROWEGO BEZPIECZEŃSTWA INFORMACJI W URZĘDZIE GMINY LIPCE REYMONTOWSKIE

1. Szkolenie z zakresu cyberbezpieczeństwa ma na celu podniesienie kompetencji kadry urzędniczej w obszarze zagrożeń teleinformatycznych, podniesienie poziomu bezpieczeństwa informacyjnego w urzędzie, poznanie prawidłowej reakcji na cyberataki, poznanie podstawowych zasad i dobrych praktyk wykorzystywania technologii informatycznych oraz zdobycie umiejętności wykorzystania tej wiedzy w praktyce.

2. Informacje dotyczące jednostki, w której szkolenie ma być przeprowadzone:

1) Liczba pracowników Urzędu objętych postępowaniem – 15 osób
2) Ilość lokalizacji działalności organizacji – 1
3) Działy w organizacji: Wójt Gminy, Skarbnik Gminy, Sekretarz Gminy, Referat Finansowy, Referat Rozwoju Gospodarki Przestrzennej i Komunalnej, Wieloosobowe stanowisko pracy do spraw Organizacyjnych i Obywatelskich, Zespół Ekonomiczno-Administracyjny Oświaty.

3. Informacje dotyczące wymagań w zakresie przeprowadzenia szkolenia:

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 pracy Urzędu Gminy.
4) Szkolenia będą prowadzone w języku polskim.
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 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. Dodatkowo, w przypadku szkoleń trwających 8 godzin zaplanowana jest przerwa trwająca 30 minut.
8) W ramach organizacji szkoleń Zamawiający zapewni:
   a) rekrutację osób biorących udział w szkoleniach,
   b) salę szkoleniową zapewniającą warunki do przeprowadzenia szkolenia,
   c) dostęp do sieci Internet.
9) W ramach organizacji szkoleń Wykonawca zapewni:
   a) materiały szkoleniowe, obejmujące szczegółowy zakres szkolenia, harmonogram dzienny szkolenia oraz materiały merytoryczne w formie papierowej, zawierające szczegółowe informacje, które będą omawiane podczas szkolenia. Materiały szkoleniowe

przekazywane są nieodpłatnie Uczestnikom na własność. 1 egzemplarz materiałów szkoleniowych zostanie przekazany Zamawiającemu w celach archiwalnych,

b) warunki pracy uczestników i Wykonawcy w trakcie trwania szkolenia zgodne przepisami bezpieczeństwa i higieny pracy,
c) oprogramowanie oraz sprzęt komputerowy umożliwiający przeprowadzenie szkolenia,
d) projektor multimedialny, tablice i inne artykuły niezbędne do prowadzenia szkoleń,
e) 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,
f) wydanie Uczestnikom szkolenia zaświadczeń o ukończeniu danego szkolenia,
g) kadrę trenerską posiadającą wiedzę i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkoleń,
h) 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.

4. 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 – pendrive 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.

5. Dodatkowe wymagania:

1) W ramach usługi zostanie przeszkolonych 15 osób w dwóch grupach.
2) Szkolenie powinno trwać minimum 4 godziny szkoleniowe dla 1 grupy szkoleniowej.