Załącznik nr 1 do zapytania ofertowego

Kowiesy, dnia 14 czerwca 2022 roku

w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożeniaREACT-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

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

CZĘŚĆ I

Wykonanie diagnozy cyberbezpieczeństwa i audytu KRI, opracowanie procedur systemów zarządzania bezpieczeństwem informacji

W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany będzie do dokonania oceny zgodności funkcjonujących zasad i procedur dotyczących zarządzania bezpieczeństwem informacji, w tym przetwarzania danych osobowych, z obowiązującymi aktami prawnymi do przeprowadzenia kompleksowego audytu bezpieczeństwa informacji w zakresie ustawowych obszarów działalności podmiotu (w tym w szczególności weryfikacji struktury organizacji oraz przepływu dokumentów, analizy zewnętrznej i wewnętrznej sieci komputerowej, analizy serwerów, testów dostępu do sieci wewnętrznej i zewnętrznej, analizy stacji roboczych, analizy kopii zapasowych, analizy poczty email, analizy ogólnego bezpieczeństwa danych i mechanizmów kontroli w podmiocie) oraz opracowania dokumentacji poaudytowej - raportu z wytycznymi do doskonalenia i rekomendacjami.

1. Diagnoza cyberbezpieczeństwa w Urzędzie Gminy Kowiesy musi zostać przeprowadzona zgodnie z Ustawą z dnia 5 lipca 2018 r. ***o krajowym systemie cyberbezpieczeństwa*** (Dz.U. z 2020 r. poz. 1369 z późn. zm.) oraz Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. ***w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*** (Dz. U. z 2017 r. poz. 2247 ze zm.) zwane dalej Rozporządzeniem KRI, w tym opracowanie raportu zawierającego wnioski i rekomendacje oraz przeprowadzenie szkolenia pracowników Urzędu w zakresie cyfrowego bezpieczeństwa informacji.
2. 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.***

3. Audyt 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 w/w rozporządzeniu:
   a) Certified Internal Auditor (CIA)
   b) Certified Information System Auditor (CISA)
   c) 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
   d) 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
   e) Certified Information Security Manager (CISM)
   f) Certified in Risk and Information Systems Control (CRISC)
   g) Certified in the Governance of Enterprise IT (CGEIT)
   h) Certified Information Systems Security Professional (CISSP)
   i) Systems Security Certified Practitioner (SSCP)
   j) CertifiedReliability Professional
   k) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert

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

<u>Załączniki do opisu diagnozy cyberbezpieczeństwa:</u>

- ✓ Formularz_informacji_związanych_z_przeprowadzeniem_diagnozy_cyberbezpieczeństwa
- ✓ Rozporządzenie Mini._Cyfryzacji_wykaz_certyfikatów_uprawniających_do_przeprowadzenia_audytu

CZĘŚĆ II

Przeprowadzenie szkolenia z zakresu cyfrowego bezpieczeństwa informacji w urzędzie gminy Kowiesy

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.

Szkolenie powinno obejmować co najmniej:

1) omówienie poprawnych zasad związanych z cyberbezpieczeństwem w Urzędzie,
2) szczegółowe informacje związane z zagrożeniami w sieci takimi jak: phishing, ransomware oraz malware i omówienie sposobów przeciwdziałania oraz zabezpieczania się przed powyższymi zagrożeniami,

Informacje dotyczące jednostki, w której szkolenie ma być przeprowadzone.

1) Liczba pracowników Urzędu objętych szkoleniem – 14 osób
2) Ilość lokalizacji działalności organizacji - 1
3) Działy w organizacji: Wójt Gminy, Skarbnik Gminy, Sekretarz Gminy, Referat Rozwoju Gospodarczego, Referat Finansowy i USC,

Informacje dotyczące wymagań w zakresie przeprowadzenia szkolenia:

Jednostką czasową szkolenia jest 1 godzina szkoleniowa (1 godzina szkolenia = 45 minut).

- Szkolenia będą trwały maksymalnie 8 godzin szkoleniowych w ciągu dnia.
- Szkolenia będą odbywać się w dni robocze w godzinach 8.00 – 16.00.
- Szkolenia będą prowadzone w języku polskim.
- Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego szczegółowego zakresu merytorycznego szkolenia oraz dziennego harmonogramu prac.
- 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.
- W ramach organizacji szkoleń Zamawiający zapewni rekrutację osób biorących udział w szkoleniach.

- 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. 1 egzemplarz materiałów szkoleniowych zostanie przekazany Zamawiającemu w celach archiwalnych,
2) salę szkoleniową (w przypadku jeżeli Zamawiający nie będzie mógł zorganizować własnej sali szkoleniowej), przystosowaną do prowadzenia zajęć dydaktycznych, zapewniającą warunki do przeprowadzenia szkolenia. Sala wyposażona będzie w wystarczającą dla wszystkich uczestników szkolenia liczbę stanowisk pracy. Sale szkoleniowe powinny być przystosowane do potrzeb osób niepełnosprawnych,
3) dostęp do sieci Internet,
4) warunki pracy uczestników i Wykonawcy w trakcie trwania szkolenia zgodne przepisami bezpieczeństwa i higieny pracy,
5) wystarczającą liczbę własnych licencji na oprogramowanie komputerowe wykorzystywane przy realizacji szkoleń oraz sprzęt komputerowy dla każdego Uczestnika umożliwiający przeprowadzenie szkolenia.
6) projektor multimedialny, tablice i inne artykuły niezbędne do prowadzenia szkoleń,
7) 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,
8) wydanie Uczestnikom szkolenia zaświadczeń o ukończeniu danego szkolenia,
9) kadrę trenerską posiadającą wiedzę i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkoleń,
10) 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.

Ramowy zakres szkolenia:

Główne założenia i wymagania prawne cyberbezpieczeństwa w pracy urzędnika.

1) Polityka bezpieczeństwa w organizacji.
2) Definicja incydentu bezpieczeństwa i zasady postępowania z incydentem.
3) 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.
4) Bezpieczeństwo fizyczne - urządzenia, dokumenty, „czyste biurko".
5) Zabezpieczenie informatycznych nośników danych – pendrivy i pamięci zewnętrzne.
6) Zdalny dostęp do zasobów jednostki i korzystanie z urządzeń prywatnych przez pracowników oraz związane z tym potencjalne zagrożenia.
7) Przechowywanie danych w chmurze i korzystanie z zewnętrznych dostawców usług informatycznych.
8) Prawidłowe korzystanie z oprogramowania antywirusowego.
9) Zasady aktualizacji programów i aplikacji.
10) Szyfrowanie dokumentów i poczty elektronicznej.
11) Polityka haseł, zarządzanie dostępem i tożsamością.

Dodatkowe wymagania:

1. W ramach usługi zostanie przeszkolonych 14 osób w dwóch grupach.
2. Szkolenie powinno odbywać się na terenie Gminy Kowiesy.
3. Szkolenie powinno trwać minimum 8 godzin szkoleniowych dla 1 grupy szkoleniowej.