Gmina Suchy Las

Załącznik nr 1 do postępowania, znak sprawy: ZP.271.7.2022

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

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 AUDYTU CTBERBEZPIECZEŃSTWA GMINY SUCHY LAS
ORAZ
PRZEPROWADZENIE SZKOLENIA Z ZAKRESU CYFROWEGO BEZPIECZEŃSTWA INFORMACJI URZĘDU GMINY SUCHY LAS

1. **Część I**.

   1.1. **Diagnoza cyberbezpieczeństwa**.

   W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany będzie do dokonania oceny zgodności funkcjonujących zasad i procedur dotyczących zarządzania bezpieczeństwem informacji oraz opracowania dokumentacji poaudytowej – raportu z wytycznymi do doskonalenia i rekomendacjami.

   1) Diagnoza cyberbezpieczeństwa musi zostać przeprowadzona zgodnie z Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560 ze 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.), w tym opracowanie raportu zawierającego wnioski i rekomendacje oraz przeprowadzenie szkolenia w zakresie cyfrowego bezpieczeństwa pracowników Urzędu.
   2) Diagnoza cyberbezpieczeństwa musi zostać wykonana zgodnie z formularzem zamieszczonym w dokumentacji konkursowej projektu Cyfrowa Gmina dostępnym na stronie internetowej 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.

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

1.2. **Szkolenie z cyfrowego bezpieczeństwa**.

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.

1. Szkolenie poaudytowe pracowników Urzędu z zakresu:

   - bezpieczeństwa pracy w systemach informatycznych, ochrony danych osobowych, legalności oprogramowania w oparciu o uzyskane wyniki audytu i testów, przedstawienie zaleceń,

   - przeprowadzenie testów penetracyjnych (przeprowadzenie kontrolowanego „ataku" na system teleinformatyczny mający na celu praktyczną ocenę bieżącego stanu bezpieczeństwa tego systemu, w szczególności obecności znanych podatności i odporności na próby przełamania zabezpieczeń),

   - przeprowadzenie testów socjotechnicznych (polegajacych na próbach uzyskania nieautoryzowanego dostępu do danych poprzez „atakowanie" pracowników - phishing, telefony itp. – w kontrolowany sposób).

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

   - liczba pracowników objeta szkoleniem – do 100 osób.

   - rekomendowana forma przeprowadzenia szkolenia: stacjonarna w siedzibie Zamawiającego/on-line.

3. Informacje dotyczące wymagań w zakresie przeprowadzenia szkolenia.

   - Wykonawca w ramach wykonania usługi przygotuje program szkolenia oraz harmonogram szkolenia i przekaże je Zamawiajacemu nie później niż 5 dni roboczych przed dniem rozpoczęcia szkolenia,

   - Wykonawca przygotuje i zapewni materiały szkoleniowe dla każdego uczestnika szkolenia, pozwalające na samodzielną edukację z zakresu objętego szkoleniem. Zamawiający dopuszcza dostarczenie dla każdego uczestnika szkolenia kompletu materiałów w formie elektronicznej, np. dokumenty w formacie PDF, w miejsce materiałów papierowych,

   - Wykonawca dostarczy uczestnikom szkolenia wyżej wymienione materiały szkoleniowe najpóźniej w dniu rozpoczęcia szkolenia,

   - wszelkie koszty opracowania materiałów szkoleniowych ponosi Wykonawca,

   - Wykonawca nie jest zobowiązany do zapewnienia uczestnikowm szkolenia wyżywienia,

   - po zakończeniu szkolenia, Wykonawca dokona ewaluacji zadowolenia uczestników oraz efektywności szkolenia,

   - Wykonawca umożliwi uczestnikom skorzystanie z konsultacji po ukończeniu szkolenia,

   - szkolenie musi być certyfikowane. Wykonawca w ramach otrzymanego wynagrodzenia zapewni uczestnikom szkolenia imienne certyfikaty potwierdzajace ukończenie szkolenia i jego zakres. Certyfikat uzyska również Urząd Gminy Suchy Las.

Załączniki do opisu diagnozy cyberbezpieczeństwa:

1. Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa – załącznik nr 8.
2. Rozporządzenie Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.