Załącznik nr 1 do SWZ - Szczegółowy opis przedmiotu zamówienia

Dotyczy zamówienia publicznego pn. Przeprowadzenie diagnozy cyberbezpieczeństwa oraz szkoleń dla pracowników z zakresu cyberbezpieczeństwa realizowanego w ramach zadania: „Dostawa, wdrożenie i integracja systemów informatycznych z dostawą sprzętu komputerowego, serwerowego i oprogramowania oraz usługami szkoleniowymi dla Gminy Susiec w ramach projektu „Cyfrowa Gmina""

Kody CPV:

- 72800000-8 Usługi audytu komputerowego i testowania komputerów
- 80510000-2 Usługi szkolenia specjalistycznego

1. **Diagnoza cyberbezpieczeństwa**
   1) **Przedmiot zamówienia.**
      Przeprowadzenie diagnozy cyberbezpieczeństwa w ramach projektu „Cyfrowa Gmina" w Urzędzie Gminy Susiec zgodnie z zakresem oraz formularzem stanowiącym załącznik nr 8 do Regulaminu Konkursu Grantowego Cyfrowa Gmina zakończonego raportem.
   2) **Szczegółowy zakres przedmiotu zamówienia zawiera formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa stanowiący załącznik nr 8 do Regulaminu Konkursu Grantowego Cyfrowa Gmina zakończonego raportem .**
   3) **O udzielenie niniejszego zamówienia mogą ubiegać się wykonawcy, którzy spełniają warunki, dotyczące:**
      Audyt musi zostać przeprowadzony przez osobę posiadająca 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 znajduje się poniżej:
      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. Certified Reliability Professional
11. Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert

4) Zamawiający dopuszcza wykonanie diagnozy w sposób zdalny.
5) Po przeprowadzeniu diagnozy, Wykonawca zobligowany jest do przekazania wypełnionego i podpisanego elektronicznie formularza diagnozy Zamawiającemu wraz z kopią certyfikatu potwierdzonej za zgodność z oryginałem uprawniającego do przeprowadzenia diagnozy .

2. Szkolenie z zakresu cyberbezpieczeństwa

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) Szkolenie powinno obejmować co najmniej:
   a) omówienie podstawowych pojęć i zasad związanych z cyberbezpieczeństwem w Urzędzie,
   b) szczegółowe informacje związane z zagrożeniami w sieci takimi jak np. phishing, ransomware, malware, socjotechnika, atak telefoniczny, spoofing, atak odwrócony - zmuszenie ofiary do szukania pomocy u atakującego, przekręt nigeryjski, wyłudzenia BLIK, oszustwo na dyrektora/prezesa + przykłady i omówienie sposobów przeciwdziałania oraz zabezpieczania się przed powyższymi zagrożeniami,
   c) metody nieautoryzowanego pozyskania danych + przykłady
   d) bezpiecznie przetwarzanie danych: szyfrowanie, przechowywanie, udostępnianie, komunikacja
   e) bezpieczne hasła, managery haseł, autoryzacja dwuetapowa, klucze sprzętowe
   f) metody obrony oraz przeciwdziałania (w tym: przed wyłudzeniem danych osobowych za pomocą metod socjotechnicznych, oprogramowaniem mogącym zablokować dostęp do urządzeń firmowych, szkodliwymi programami mogącymi pozyskać dane firmowe lub osobiste)
   g) bezpieczne korzystanie ze smartfonów
   h) wskazanie zasad cyberhigieny
3) Informacje dotyczące jednostki, w której szkolenie ma być przeprowadzone.
   a) Liczba pracowników Urzędu objętych postępowaniem – 27 osób
   b) Szkolenie będzie przeznaczone dla wszystkich pracowników Urzędu Gminy w Suścu (27 osób). Szkolenie odbędzie się w 2 turach po ok. 19 pracowników na każdą z tur. Szkolenie zostanie przeprowadzone z uwzględnieniem faktu, że uczestnicy szkolenia mogą nie posiadać wiedzy informatycznej i technicznej.
   c) Ilość lokalizacji działalności organizacji-1.
   d) Czas trwania szkolenia – min. 3,5 godz na grupę.
4) Wykonawca w ramach wykonania usługi przygotuje harmonogram szkolenia oraz program szkolenia i dostarczy je w terminie nie później niż 7 dni roboczych przed dniem rozpoczęcia szkolenia do akceptacji przez Zamawiającego. Harmonogram zajęć powinien zawierać informacje dotyczące czasu i miejsca realizacji danego szkolenia.
5) Wykonawca przygotuje i zapewni materiały szkoleniowe dla każdego uczestnika szkolenia, pozwalające na samodzielną edukację z zakresu tematyki szkolenia (np. opracowania, wydruki materiałów szkoleniowych). Zamawiający dopuszcza dostarczenie dla każdego

uczestnika szkolenia kompletu materiałów w formie elektronicznej, np. dokumenty w standardzie PDF, w miejsce materiałów papierowych.

6) Wykonawca dostarczy uczestnikom szkolenia ww. materiały szkoleniowe najpóźniej w dniu rozpoczęcia szkolenia.
7) Wykonawca przygotuje również dla zamawiającego materiały ze szkolenia, które będzie mógł wykorzystać do przeszkolenia nieobecnych lub nowych pracowników.
8) Wszelkie koszty opracowania materiałów szkoleniowych ponosi Wykonawca.
9) Wykonawca zorganizuje szkolenie w siedzibie zamawiającego.
10) W przypadku wprowadzenia obostrzeń związanych z pandemią dopuszcza się możliwość szkolenia zdalnego, wówczas wykonawca zapewni oprogramowanie do jego przeprowadzenia.
    a) Oprogramowanie wykorzystane do udostępnienia ekranu komputera prowadzącego, obrazu oraz dźwięku z sali szkoleniowej zostanie udostępnione uczestnikom szkolenia bez ponoszenia przez Zamawiającego dodatkowych kosztów. Wykorzystane oprogramowanie będzie pochodzić z legalnego źródła oraz sposób użycia nie może naruszać warunków licencyjnych, na jakich oprogramowanie zostało udostępnione.
    b) Wykorzystane oprogramowanie musi umożliwiać uczestnikom szkolenia zadawanie pytań i zgłaszanie wątpliwości w czasie rzeczywistym.
    c) Sposób prowadzenia szkolenia przez prowadzącego musi umożliwiać uczestnikom zadawanie pytań i zgłaszanie wątpliwości w czasie rzeczywistym.
11) Wykonawca nie jest zobowiązany do zapewnienia uczestnikom szkolenia wyżywienia.
12) Po przeprowadzonym szkoleniu Wykonawca dokonuje ewaluacji zadowolenia uczestników oraz efektywności szkolenia.
13) Szkolenie musi być certyfikowane. Wykonawca w ramach otrzymanego wynagrodzenia zapewni uczestnikom szkolenia imienne certyfikaty potwierdzające ukończenie szkolenia i jego zakres.