Załącznik nr 1 do Zapytania ofertowego znak 271.10.27.2022

Szczegółowy Opis Przedmiotu Zamówienia

na przeprowadzenie diagnozy cyberbezpieczeństwa oraz szkoleń w zakresie cyberbezpieczeństwa

Spis treści

1. Zestawienie ilościowe 2
2. Opis przedmiotu zamówienia 2
   2.1. Przeprowadzenie szkolenia w zakresie cyberbezpieczeństwa. 2
      2.1.1. Wymagania ogólne dla szkoleń: 2
      2.1.2. Wymagana agenda szkolenia: 2
   Szkolenie – cyberbezpieczeństwo oraz zagrożenia w cyberprzestrzeni. 2
   2.2. Przeprowadzenie diagnozy cyberbezpieczeństwa. 4
   2.3. Przeprowadzenie audytu zgodności z Krajowymi Ramami Interoperacyjności 4

1. Zestawienie ilościowe.

Przedmiot zamówienia obejmuje przeprowadzenie diagnozy cyberbezpieczeństwa oraz szkoleń z zakresu cyberbezpieczeństwa

Lp.	Nazwa	Ilość
1.	Przeprowadzenie szkolenia dla pracowników w zakresie cyberbezpieczeństwa	Liczba osób 28
2.	Przeprowadzenie diagnozy cyberbezpieczeństwa	1 szt.
3	Przeprowadzenie audytu KRI	1 szt.

2. Opis przedmiotu zamówienia

2.1. Przeprowadzenie szkolenia w zakresie cyberbezpieczeństwa.

2.1.1. Wymagania ogólne dla szkoleń:

1. Szkolenie musi odbyć się w siedzibie Zamawiającego ale Wykonawca powinien również dostarczyć platformę umożliwiającą prowadzenie szkoleń i być gotowym do organizacji szkolenia online.
2. Zamawiający udostępni bezpłatnie pomieszczenie wyposażone w rzutnik oraz dostęp do Internetu, na potrzeby szkolenia stacjonarnego.
3. Szkolenie powinno trwać do 2 godzin szkoleniowych dla 1 grupy szkoleniowej w ciągu dnia.
4. Szkolenia będą odbywać się w dni robocze od poniedziałku do piątku w godzinach 7.30 – 15.30.
5. W celu maksymalizacji czasu nie przewiduje się przerw podczas szkolenia.
6. W ramach organizacji szkoleń Wykonawca zapewni:
   1) Materiały szkoleniowe dla każdego uczestnika szkolenia w postaci elektronicznej, które Zamawiający będzie mógł wykorzystać nieodpłatnie i wydrukować dla każdego uczestnika. Materiały muszą zawierać szczegółowe informacje, które będą omawiane podczas szkolenia.
   2) Wydanie Uczestnikom szkolenia zaświadczeń o ukończeniu danego szkolenia.
   3) 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) Ankieta satysfakcji ze szkolenia.
   4) Test wiedzy dotyczący przedmiotu szkolenia realizowany w trybie on-line.

2.1.2. Wymagana agenda szkolenia:

Szkolenie – cyberbezpieczeństwo oraz zagrożenia w cyberprzestrzeni.

Temat szkolenia
Głównym tematem szkolenia będzie omówienie poprawnych zasad związanych z cyberbezpieczeństwem. Ponadto zostaną omówione zagrożenia w sieci takie jak phishing, ransomware oraz malware, które powodują w dobie Internetu poważne zagrożenia dla Państwa firmy oraz pracowników.

Na szkoleniu poruszone zostaną również sposoby przeciwdziałania oraz zabezpieczania się przed powyższymi zagrożeniami, co w stopniu wyższym podniesie wiedzę Państwa firmy z zakresu cyberbezpieczeństwa.

Agenda

1. Czym jest cyberbezpieczeńtwo i dlaczego jest tak ważne w dzisiejszych czasach?
2. Omówienie najczęściej występujących metod nieautoryzowanego pozyskania danych oraz występujących zagrożeń poparte przykładami z Polski i ze Świata.
   - Czym jest phishing?
   - Czym jest ransoware?
   - Czym jest malware?
   - Ciekawość to pierwszy stopień do piekła.
3. Omówienie metod obrony oraz przeciwdziałania przed:
   - Wyłudzeniem danych osobowych za pomocą technik socjotechnicznych (phishing).
   - Oprogramowaniem mogącym zablokować dostęp do urządzeń firmowych wraz z plikami znajdującymi się na tych urządzeniach (ransoware).
   - Szkodliwymi programami mogącymi pozyskać dane firmowe oraz osobiste pracowników (malware).
   - Ciekawością pracowników podczas wykonywania ich obowiązków służbowych (czynnik ludzki).
4. Omówienie informacji, które należy chronić.
5. Omówienie 10 zasad bezpieczeństwa informacji
6. Omówienie 10 zasad zarządzania hasłami
7. Omówienie stosowania managerów haseł.
8. Omówienie ścieżki postępowania w przypadku naruszenia bezpieczeństwa.

2.2. Przeprowadzenie diagnozy cyberbezpieczeństwa.

1. 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).
2. 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.
3. 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.

2.3. Przeprowadzenie audytu zgodności z Krajowymi Ramami Interoperacyjności

1. Audyt winien być wykonany na zgodność z 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.
2. Audyt powinien być zrealizowany w oparciu o Wytyczne dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych Załącznik nr 1.
3. Wykonawca przedstawi wynik audytu w postaci zestawienia sprawdzeń oraz zestawu zaleceń umożliwiających minimalizację zidentyfikowanych ryzyk.