Załącznik nr 2 do SWZ

**Szczegółowy Opis Przedmiotu Zamówienia**

**Przeprowadzenie szkoleń z obsługi sprzętu komputerowego, cyberbezpieczeństwa oraz przeprowadzenie audytów oraz testów penetracyjnych systemów informatycznych w ramach projektu ,,Cyfrowa Gmina”**

**Zadanie 1. Szkolenie stacjonarne dla pracowników Urzędu Miasta i Gminy w Chmielniku w zakresie obsługi oprogramowania**

1) Szkolenie zostanie przeprowadzone w formie stacjonarnej (w siedzibie Zamawiającego) prezentacji i wykładu dla dwóch osobnych grup maksymalnie do 30 osobowych;

2) Czas trwania szkolenia dla każdej z grup - do 1,5h + 30min (ewentualna dyskusja i zadawanie pytań);

3) Tematyka szkolenia będzie dotyczyła min. zagadnień z zakresu:  
- obsługi pakietu biurowego: WORD, Excel,   
- wysyłki poczty elektronicznej,   
- szyfrowania dokumentów WORD, Excel, pdf, tworzenia dokumentu do pliku pdf,

**Termin realizacji: listopad 2022 r.**

**Zadanie nr 2. Szkolenie dla pracowników Urzędu Miasta i Gminy w Chmielniku w zakresie cyberbezpieczeństwa**

1) Szkolenie zostanie przeprowadzone w formie stacjonarnej (w siedzibie klienta) prezentacji i wykładu dla dwóch osobnych grup maksymalnie do 30 osobowych;

2) Czas trwania szkolenia dla każdej z grup - do 1,5h + 30min (ewentualna dyskusja i zadawanie pytań);

3) Tematyka szkolenia będzie dotyczyła min. zagadnień z zakresu cyberbezpieczeństwa tj. :

- ochrona danych osobowych,

- zagrożenia dla użytkownika i zasobów organizacji;

- socjotechniczne mechanizmy działania cyberprzestępców;

- rozpoznawanie zagrożeń oraz reagowanie na pojawiające się niebezpieczeństwa;

- dobre praktyki zabezpieczania się przed poszczególnymi zagrożeniami;

- utrzymanie bezpieczeństwa informacji w systemach informatycznych (zabezpieczanie środowiska pracy)

- podstawy bezpieczeństwa systemów informatycznych;

- przenoszenie się zagrożeń pomiędzy obszarem prywatnym a służbowym;

- profilaktyka bezpiecznego korzystania z Internetu oraz sieci LAN i Wi-Fi,

- konsekwencje lekceważenia zasad cybezpieczeństwa;

4) Do dyspozycji zamawiającego zostaną przekazane w formie elektronicznej materiały obejmujące tematykę szkolenia.

5) Wykonawca oświadcza, że posiada potencjał techniczny, osobowy, wiedzę oraz doświadczenie niezbędne do wykonania przedmiotu zamówienia – konieczne wykazanie przez wykonawcę, że w okresie ostatnich 3 lat wykonywane były przez niego szkolenia z zakresu cyberbezpieczeństwa lub bezpieczeństwa pracy w systemach informatycznych, w co najmniej 6 jednostkach samorządu terytorialnego.

**Termin realizacji:**  
**1. Szkolenie nr 1 – październik 2022 r.  
2. Szkolenie nr 2 – luty 2023 r.**

**Zadanie nr 3. Przeprowadzenie audytów w jednostce zgodności z KRI i RODO**

Przeprowadzenie dwóch audytów - ocenę dostosowania systemu zarządzania bezpieczeństwa informacji w Urzędzie Miasta i Gminy w Chmielniku do wymagań Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (KRI) (t.j. Dz.U. z 2017 r., poz. 2247), Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560 z późn. zm.). w tym legalności oprogramowania, testy penetracyjne, audyt bezpieczeństwa informacji, ocenę dostosowania systemu zarządzania bezpieczeństwa informacji w Urzędzie Miasta   
i Gminy w Chmielniku do wymagań RODO;

2/ W oparciu o raport z audytu przedstawienie rekomendacji dostosowującej stosowną dokumentację Systemu Zarządzania Bezpieczeństwem Informacji do spełnienia wymogów KRI, RODO oraz PN-ISO/IEC 27001 lub późniejszej.

**Audyt (przegląd i ocena)**

Cel audytu

Audyt w Urzędzie Miasta i Gminy w Chmielniku, którego celem jest:

1. Weryfikacja poziomu spełnienia wymagań Rozporządzenia Rady Ministrów z dnia   
   12 kwietnia 2012 w sprawie KRI, minimalnych wymagań dla rejestrów publicznych   
   i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych w Urzędzie Miasta i Gminy w Chmielniku,
2. Weryfikacja poziomu spełnienia wymagań pod kątem zgodności z polską normą PN-ISO/IEC 27001 lub późniejszej, w tym ocena skuteczności funkcjonujących zabezpieczeń technicznych, organizacyjnych i prawnych.

Audyt dotyczy:   
Ilość lokalizacji: 2 lokalizacje (jedna główna i jedna zamiejscowa: 4stanowiska)  
Ilość pracowników przetwarzających dane: do 50.  
Ilość stanowisk komputerowych: do 65.  
Ilość serwerów (fizycznych i wirtualnych): 5 fizycznych, 1 wirtualny.  
Ilość systemów przetwarzających dane: 17.  
Ilość serwerowni:1 serwerownia.  
Ilość urządzeń sieciowych – (drukarki, routery, switche, przełączniki, urządzenia VoIP etc.) - drukarki-30, routery -2, switche-7, przełączniki-6, VoIP- nie ma.  
Access Point: 3.  
Ilość drukarek sieciowych: 10  
Ilość podsieci: nie ma  
Ilość adresów zewnętrznych: 3.

*Audyt (przegląd i ocena) nie ma charakteru uzyskiwania certyfikatu zgodności ww. systemu zarządzania bezpieczeństwa informacji z Polską Normą PN-ISO/IEC 27001 lub późniejszą.*

*W postępowaniu nie mogą brać udziału podmioty, z którymi, w czasie postępowania ofertowego, Zamawiający ma podpisane klauzule lub umowy o powierzeniu danych osobowych*

**Termin realizacji zamówienia:**

**1. Audyt nr 1 w roku 2022 w październiku,**

**2. Audyt nr 2 w roku 2023 r. lutym,**

**Zadanie nr 4. Przeprowadzenie testów penetracyjnych systemów informatycznych JST**

Ilość lokalizacji: 2 lokalizacje (jedna główna i jedna zamiejscowa: 4 stanowiska)  
Ilość pracowników przetwarzających dane: do 50.  
Ilość stanowisk komputerowych: do 65.  
Ilość serwerów (fizycznych i wirtualnych): 5 fizycznych, 1 wirtualny.  
Ilość systemów przetwarzających dane: 17.  
Ilość serwerowni:1 serwerownia.  
Ilość urządzeń sieciowych – (drukarki, routery, switche, przełączniki, urządzenia VoIP etc.) - drukarki-30, routery -2, switche-7, przełączniki-6, VoIP- nie ma.  
Access Point: 3.  
Ilość drukarek sieciowych: 10  
Ilość podsieci: nie ma  
Ilość adresów zewnętrznych: 3.

Zewnętrzne i wewnętrzne testy penetracyjne infrastruktury informatycznej  
Testy styku sieci lokalnej z internetem przeprowadzane ze stacji roboczej podłączonej do sieci internet  
Analiza topologii brzegu sieci;  
Weryfikacja mechanizmów ochronnych;  
Próba wykrycia usług sieciowych udostępnianych do internetu;  
Detekcja wersji oraz typu oprogramowania dostępnego z sieci internet;  
Exploitacja dostępnych urządzeń oraz usług wystawionych do sieci internet;  
Przedstawienie rozwiązań zwiększających bezpieczeństw styku sieci lokalnej z siecią internet.

Testy penetracyjne przeprowadzone ze stacji roboczej podłączonej do wewnętrznego systemu informatycznego w celu zidentyfikowania możliwości przeprowadzenia włamania z wewnątrz organizacji  
Analiza topologii sieci LAN;  
Weryfikacja mechanizmów ochronnych w sieci;  
Analiza komunikacji sieciowej;  
Skanowanie portów TCP/UDP próba wykrycia usług sieciowych;  
Skanowanie hostów aktywnych w sieci;  
Exploitacja dostępnych urządzeń oraz usług w sieci LAN;  
Przedstawienie rozwiązań zwiększających bezpieczeństw sieci LAN.

*Posiadanie wersji komercyjnej oprogramowania niezbędnego do wykonania Audytu Bezpieczeństwa Sieci*

*W postępowaniu nie mogą brać udziału podmioty, z którymi, w czasie postępowania ofertowego, Zamawiający ma podpisane klauzule lub umowy o powierzeniu danych osobowych.*

**Termin realizacji zamówienia:**

1. Test nr 1 w roku 2022 w październiku,

2. Test nr 2 w roku 2023 r. w lutym,