Specyfikacja szkolenia z cyberbezpieczeństwa dla pracowników z zapewnionym sprzętem przez firmę szkoleniową, podzielone na 4-6 grup o wielkości od 12 do 15 osób.

Cele szkolenia:

1. Zapoznanie uczestników z podstawowymi zagadnieniami z zakresu cyberbezpieczeństwa w pracy urzędnika.
2. Przekazanie informacji na temat różnych rodzajów ataków oraz skutecznych metod ich zapobiegania.
3. Nauczenie uczestników o najważniejszych zasadach bezpieczeństwa w pracy z komputerami, sieciami, aplikacjami i danymi.
4. Rozwijanie świadomości w zakresie zagrożeń związanych z korzystaniem z urządzeń prywatnych i chmury.
5. Praktyczne ćwiczenia i studia przypadków, które umożliwią uczestnikom zastosowanie zdobytej wiedzy w praktyce.

Agenda szkolenia:

- Wprowadzenie do cyberbezpieczeństwa dla urzędników: znaczenie, założenia prawne, polityka bezpieczeństwa.
- Rodzaje ataków w cyberprzestrzeni: socjotechnika, ataki komputerowe, phishing, spam, itp.
- Bezpieczeństwo fizyczne i „czyste biurko": ochrona urządzeń i dokumentów.
- Bezpieczeństwo stacji roboczych: zabezpieczenia, aktualizacje, oprogramowanie antywirusowe
- Ćwiczenia praktyczne: identyfikacja zagrożeń, rozpoznawanie phishingu.
- Bezpieczne korzystanie z urządzeń zewnętrznych: pendrive, pamięci zewnętrzne.
- Zdalny dostęp do zasobów jednostki i korzystanie z urządzeń prywatnych: zagrożenia i zabezpieczenia.
- Bezpieczeństwo w chmurze: przechowywanie danych, dostawcy usług.
- Szyfrowanie dokumentów i poczty elektronicznej.
- Bezpieczeństwo sieci LAN i Wi-Fi.
- Ćwiczenia praktyczne: zabezpieczanie urządzeń zewnętrznych, konfiguracja sieci bezprzewodowych.
- Bezpieczeństwo aplikacji ministerialnych i wewnątrzorganizacyjnych.
- Zarządzanie tożsamością w internecie i wewnątrz organizacji.
- Bezpieczeństwo baz danych i infrastruktury.
- Bezpieczeństwo mobilne: zasady ochrony urządzeń mobilnych i danych.
- Ćwiczenia praktyczne: analiza przypadków, tworzenie polityki haseł, zarządzanie dostępem.

Wymagania:

- Laptopy dla uczestników szkolenia (przynajmniej 1 laptop na 2 osoby),
- Tablica lub flipchart do zapisywania notatek i prowadzenia dyskusji,
- Sprzęt do praktycznych ćwiczeń, takich jak pendrive, pamięci zewnętrzne, urządzenia mobilne, w zależności od tematyki szkolenia,
- Certyfikaty:

a) Offensive Security Certified Professional (OSCP)
b) Offensive Security Certified Expert (OSCE)

Przed podpisaniem umowy wybrany Wykonawca przedłoży kserokopie certyfikatów, potwierdzających posiadanie uprawnień, kwalifikacji zawodowych przez osoby uczestniczące w wykonaniu zamówienia.
Firma szkoleniowa będzie odpowiedzialna za zapewnienie wymaganego sprzętu, jego konfigurację przed rozpoczęciem szkolenia oraz sprawdzenie jego sprawności. Instruktorzy będą również dostarczać niezbędne materiały szkoleniowe w formie elektronicznej lub wydrukowanej, które uczestnicy będą mogli wykorzystać podczas szkolenia i jako podręczniki do dalszej nauki.

Dodatkowo, firma szkoleniowa będzie miała personel techniczny gotowy do udzielenia pomocy w przypadku jakichkolwiek problemów technicznych podczas trwania szkolenia.