IZP.272.37.2025

ZAŁ. NR 6 - OPIS PRZEDMIOTU ZAMÓWIENIA

Część 2: Szkolenie z zakresu cyberbezpieczeństwa dla wybranych przedstawicieli kadry JST, istotnych z punktu widzenia wdrażanej PBI i SZBI

Forma szkolenia: on-line

1. Szkolenie zostanie przeprowadzone w formie on-line dla jednej grupy szkoleniowej.
2. Jednostką czasową szkolenia jest 1 godzina szkoleniowa (45 minut).
3. Szkolenie odbędzie się w ustalonym dniu roboczym, rozpoczęcie nie wcześniej niż 8.00, zakończenie nie później niż 15:30, w terminie uzgodnionym z Zamawiającym.
4. Szkolenie będzie prowadzone w języku polskim.
5. Szkolenie prowadzone będzie na podstawie zaakceptowanego przez Zamawiającego harmonogramu zawierającego zakres merytoryczny, dostarczonego przez Wykonawcę Zamawiającemu przed podpisaniem umowy.
6. Szkolenie musi być na każdym etapie zgodne z zasadami: równości szans i niedyskryminacji, w tym dostępności dla osób z niepełnosprawnościami oraz równości kobiet i mężczyzn.
7. Usługa szkolenia elektronicznego on-line, świadczona przez usługodawcę, musi być dostępna dla wszystkich, bez względu na ich płeć, wiek, pochodzenie, orientację seksualną, niepełnosprawność czy inne przesłanki dyskryminacji.

Liczba szkolonych osób: 14

Minimalne wymagania: Szkolenie w wymiarze min. 6 godz. szkoleniowych w języku polskim

Szkolenie ma uwzględniać co najmniej następujące tematy:

1. Wprowadzenie do tematyki związanej z ochroną przed cyberzagrożeniami. Bezpieczeństwo informacji w świetle rozwijających się technologii
2. Budowa Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) - wymagania dokumentacyjne. System zarządzania bezpieczeństwem informacji – wymagania wynikające z ISO/IEC 27001, cyberbezpieczeństwo. Kluczowe obszary.
3. Przegląd zagrożeń dla bezpieczeństwa informacji przetwarzanych w formie tradycyjnej oraz elektronicznej.
4. Źródła zagrożeń związanych z bezpieczeństwem informacji oraz ich klasyfikacja w oparciu o możliwe zdarzenia i straty dla organizacji.
5. Zarządzanie ryzykiem - podejście praktyczne.
6. Najczęstsze praktyki i sposoby wyłudzania, oszustw lub kradzieży informacji z organizacji:
   a) wykradanie danych,
   b) phishing i zaawansowane techniki wykorzystywane przez cyberprzestępców,
   c) ataki socjotechniczne,
   d) malware,
   e) kontrola dostępu,
   f) działania pracowników wewnętrznych na szkodę organizacji,
   g) techniki manipulacji,
   h) biały wywiad,

i) ataki destrukcyjne,
j) atak ukierunkowane (Advanced Persistent Threat - APT) na osoby zarządzające.

7. Do czego może doprowadzić SPAM ?
8. Zarządzanie aktywami informacyjnym.
9. Proces autoryzacji urządzeń mobilnych.
10. Wykorzystywanie sprzętu prywatnego do celów służbowych ?
    a) model BYOD (bring your won device) - pracownicy korzystają z własnych urządzeń mobilnych także w celach służbowych
    b) model COPE (corporate owned personal enable) - używany przez pracowników sprzęt jest własnością przedsiębiorstwa i to ono wybiera, z czego pracownicy będą korzystać
    c) model CYOD (choose your own device) - firma tworzy listę urządzeń mobilnych, które może zapewnić swoim pracownikom.
11. Najlepsze praktyki w zakresie cyberbezpieczeństwa:
    a) Zarządzanie dostępem do sieci i systemów IT,
    b) Korzystanie z sieci bezprzewodowych w pracy i w domu,
    c) Praca zdalna - ryzyka, rekomendacje,
    d) Zarządzanie hasłami,
    e) Wdrażania silnych mechanizmów ochrony przed kradzieżą sprzętu i tożsamości oraz nieautoryzowanym dostępem do zasobów organizacji,
    f) Dostęp uprzywilejowany,
    g) Polityka czystego biurka i czystego ekranu.
12. Korzystanie z urządzeń końcowych nagrywających dźwięk i obraz.
13. Obsługa incydentów. Tworzenie schematu postępowania zarządzania incydentami.
14. Rola pracownika w doskonaleniu ochrony oraz postępowanie z najczęstszymi incydentami związanymi z bezpieczeństwem informacji.
15. Najczęstsze problemy zidentyfikowane w trakcie odbytych audytów z zakresu bezpieczeństwa.

Po szkoleniu kursant otrzymuje:

1. Zaświadczenie ukończenia szkolenia.
2. Materiały szkoleniowe.

Wymaganie dotyczące Wykonawcy:

- Wykonawca powinien posiadać stosowną wiedzę oraz min. 3 letnie doświadczenie w przygotowaniu i przeprowadzeniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń oraz w zakresie SZBI.

Termin realizacji:

- do dnia 30.09.2025 r.