SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

PRZEPROWADZENIE SZKOLEŃ zgodnie z następującymi wymaganiami:

1) SZKOLENIE DLA UŻYTKOWNIKÓW KOŃCOWYCH

– tryb zdalny PLATFORMA e-LEARNING - przeprowadzić szkolenia pracowników urzędu z zakresu CYBERBEZPIECZEŃSTWA IT (ze szczególnym uwzględnieniem współczesnych metod hakerskich i stosowanych socjotechnik oraz jak się przed tym skutecznie bronić i jak postępować z incydentem)

Szkolenie ma być podane w ciekawej i przyjaznej formie, a jednocześnie z uwzględnieniem obowiązujących przepisów prawa:
- Ogólnego Rozporządzenia o Ochronie Danych Osobowych (RODO art.39 pkt.1b)
- Ustawie o Krajowym Systemie Cyberbezpieczeństwa (KSC art.69 pkt.2)
- Rozporządzeniu Rady Ministrów w sprawie Krajowych Ram Interoperacyjności (KRI par.20 pkt.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.

W związku z tym aby nie dochodziło do dyskryminacji i wykluczenia przy organizacji szkoleń w tym projekcie uwzględniono pracowników zarówno dydaktycznych jak i administracyjnych bez względu na płeć, ponadto zaplanowane szkolenia będą prowadzone w przyjaznej formie online która nie wykluczy osób z niepełnosprawnościami np. poprzez udostępnienie alternatywnych formatów np. w formie audio lub napisów.

Usługa szkolenia elektronicznego świadczona przez usługodawcę musi być dostępna dla wszystkich, bez względu na ich płeć, wiek, pochodzenie, orientację seksualną, niepełnosprawność czy inne przesłanki dyskryminacji.

Wykonawca dostarczy materiały informacyjne i promocyjne na temat szkolenia elektronicznego które zostaną przekazane uczestnikom tych szkoleń. (Działania takie zachęcą uczestników do czynnego udziału w szkoleniach)

Szkolenie zrealizowane ma być łącznie **dla 250 osób**. Wykonane w trybie e-Learning. Wykaz imienny uczestników wraz z adresami e-mail zostanie przekazany Wykonawcy wyłonionym w niniejszym postępowaniu na etapie podpisywania umowy. Zamawiający przewiduje również alternatywną formę aktywacji kont na platformie szkoleniowej e-Learning na podstawie wcześniej utworzonych anonimowych danych startowych które w procesie rejestracji zostaną spersonalizowane przez uczestników szkolenia.

Opis szczegółowy usługi szkoleń elektronicznych z zakresu bezpieczeństwa teleinformatycznego i danych osobowych:

1. **Przedmiot zamówienia:** Usługa na szkolenie w wersji elektronicznej (e-learning) z zakresu bezpieczeństwa informacji i bezpieczeństwa teleinformatycznego. Szkolenia dedykowane dla pracowników biurowych (nietechnicznych) pracujących z komputerami i przetwarzających różnego rodzaju informacje o różnym poziomie poufności.
   Szkolenie zostanie udostępnione **dla 250 uczestników** na okres **do dnia 30 czerwca 2025 r.**
   Świadczenie usługi szkolenia musi obejmować: utworzenie indywidualnych kont dla pracowników, przesłanie danych dostępowych dla każdego pracownika przez email, świadczenie usług wsparcia technicznego dla uczestników szkolenia poprzez email oraz szczegółowe raportowanie aktywności uczestników na szkoleniu, z uwzględnieniem informacji o ukończeniu poszczególnych lekcji, wyniku testu końcowego. Częstotliwość dostarczania raportu minimum 1 raz na tydzień.

2. **Forma e-learning:** Szkolenie musi być w postaci oddzielnych lekcji dla każdej z kategorii z niżej opisanego zakresu. Szkolenie powinno zawierać minimum 30 slajdów dla jednej lekcji. Czas jednej lekcji (tematu) powinien oscylować w granicach 20-30 min. Lekcje powinny być multimedialne z wykorzystaniem scenek rodzajowych z możliwością odtworzenia w postaci dźwiękowej z użyciem lektora. Nie mogą to być same zdjęcia, definicje lub zagadnienia opisane w formie tekstowej i odtwarzane w postaci dźwiękowej. Podczas lekcji powinna być na bieżąco weryfikowana wiedza (uwaga) użytkownika poprzez np. ćwiczenia sprawdzające.

3. Zakres tematyczny szkolenia : Szkolenie musi posiadać oddzielne lekcje dla co najmniej następujących zagadnień:

Zakres tematyczny dla CYBERBEZPIECZEŃSTWO:

1. Czym jest bezpieczeństwo informacji;
2. Aspekty prawne związane z bezpieczeństwem informacji;
3. Czym jest phishing?
4. Zasady korzystania z Internetu;
5. Zasady korzystania z portali społecznościowych;
6. Zasady korzystania z poczty elektronicznej i zagrożenia z tym związane;
7. Zasady korzystania z bezpiecznych haseł;
8. Zagrożenia i sposoby zabezpieczania sprzętu mobilnego;
9. Metody pozyskiwania informacji (socjotechnika);
10. Bezpieczeństwo w zakresie płatności elektronicznych;
11. Bezpieczeństwo fizyczne w zakresie zabezpieczania pomieszczeń, dokumentacji, sprzętu IT;
12. Czym jest ransomware i jak wygląda w praktyce;
13. Jak bezpiecznie korzystać z menedżera haseł w praktyce;

14. Techniki stosowane przez cyberprzestępców;
15. Uważaj by nie zostać „mułem finansowym”
16. Bezprzewodowe życie.
17. Praca zdalna - jak zrealizować ją bezpiecznie?
18. Vishing… co to jest?
19. Phishing – stare problemy, nowe sposoby. Przykłady aktualnych cyberataków i sposoby ochrony przed nimi.
20. Jak cyberprzestępcy kradną dane przez telefon.
21. Fake news i dezinformacja.
22. Jak zapewnić ciągłość działania.
23. Cloud. O co chodzi w chmurach obliczeniowych?
24. Test z imiennym certyfikatem ukończenia kursu.

4. Forma szkolenia:

Szkolenie musi posiadać atrakcyjną formę przekazu materiału, zachęcającą osoby uczące się do aktywnego odbywania szkolenia. Zamawiający wymaga atrakcyjnej formy przekazu materiału szkolenia. Atrakcyjna forma to m.in. grafika oparta na scenkach, postaciach, dialogach, przykładach, ćwiczeniach, testach sprawdzających wiedzę oraz dźwięk – głos lektorów indywidualny dla każdej z postaci występujących w szkoleniu.

Szkolenie musi posiadać interaktywną formę, zwiększającą zaangażowanie osób uczących się. Szkolenie musi zostać wyposażone w elementy interakcji (np. kliknięcia, ćwiczenia), tak aby uczestnik był aktywny podczas szkolenia i nie miał możliwości zaliczenia szkolenia w sposób bierny tj. poprzez samoczynne odtworzenia filmu/ szkolenia.

Lekcje szkolenia muszą kłaść duży nacisk na umiejętności praktyczne, nie tylko teorię bezpieczeństwa IT. W celu zwiększenia praktycznej przydatności szkolenia musi ono zostać opracowane tak, aby zajęcia kładły większy nacisk na umiejętności praktyczne użytkowników komputerów (np. wykrywanie sytuacji zagrożenia w trakcie korzystania z serwisów społecznościowych, właściwe postępowanie w razie incydentu) niż samą teorię bezpieczeństwa IT.

Cały materiał szkolenia musi być dostępny w języku polskim i przedstawiony w sposób zrozumiały przez osoby nietechniczne.

Szkolenie musi posiadać wysoką jakość merytoryczną przygotowanego scenariusza. Scenariusz szkolenia musi zostać opracowany we współpracy z ekspertem bezpieczeństwa IT posiadającym certyfikat Lead Auditor 27001.

5. Wymagania techniczne: Szkolenie musi być wykonane w technologii HTML5. Szkolenie musi być podzielone tematycznie w taki sposób, aby można było operować (zarządzać dostępnością, harmonogramem, itp.) poszczególnymi tematami z osobna. Dostępność szkolenia 24/7. Obsługa interfejsu platformy szkoleniowej musi być dostępna w języku polskim.

6. **Czas realizacji usługi : do dnia 30 czerwca 2025 r.** W celach rozliczeniowych szkolenie nie może zakończyć się później niż okres realizacji projektu Cyberbezpieczny Samorząd.
   Zakres tematyczny powinien być podzielony na maksymalnie 4 kampanie (kilka lekcji w kampanii) zakończonych testem z imiennym certyfikatem ukończenia kursu.

7. **Termin realizacji** - uruchomienia usługi: 14 dni od daty zawarcia umowy.

2) SZKOLENIE DLA Kadry Kierowniczej

– Szkolenia dla pracowników Urzędu Miasta Łomża w zakresie bezpieczeństwa informacji mają obejmować odpowiednio:
a) Szkolenie z zakresu bezpieczeństwa informacji w Urzędzie Miasta Łomży zostanie przeprowadzone w formie stacjonarnej w siedzibie Zamawiającego dla **30 uczestników**
b) Jednostką czasową szkolenia jest 1 godzina szkoleniowa (45 minut).
c) Szkolenia będą trwały minimum 6 godzin
d) Szkolenia będą odbywać się w dni robocze w godzinach 8.00 – 16.00.
e) Szkolenia będą prowadzone w języku polskim.
f) Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego harmonogramu zawierającego zakres merytoryczny, dostarczonego przez Wykonawcę Zamawiającemu przed podpisaniem umowy.

Szczegółowy opis przedmiotu zamówienia:
Organizacja i przeprowadzenie szkolenia:

Tematyka szkolenia będzie dotyczyła w szczególności następujących zagadnień z zakresu bezpieczeństwa informacji:

1. Wprowadzenie do tematyki związanej z ochroną przed cyberzagrożeniami. Bezpieczeństwo informacji w świetle rozwijających się technologii
2. System zarządzania bezpieczeństwem informacji wynikających z ISO/IEC 27001, a cyberbezpieczeństwo. Kluczowe obszary.
3. Przegląd zagrożeń dla bezpieczeństwa informacji przetwarzanych formą tradycyjną oraz elektroniczną.
4. Źródła zagrożeń związanych z bezpieczeństwem informacji oraz ich klasyfikacja w oparciu o możliwe zdarzenia i straty dla organizacji.
5. Zarządzanie ryzykiem, jako kluczowy element ochrony. Podejście praktyczne.
6. Najczęstsze praktyki i sposoby wyłudzania, oszustw lub kradzieży informacji z organizacji:
   - wykradanie danych,
   - phishing i zaawansowane techniki wykorzystywane przez cyberprzestępców,
   - ataki socjotechniczne,
   - malware,
   - kontrola dostępu,
   - działania pracowników wewnętrznych na szkodę organizacji
   - techniki manipulacji,
   - biały wywiad,

- ataki destrukcyjne.

7. Case study: atak ukierunkowany (APT) na osoby zarządzające i zbudowanie roadmapy ataku.
8. Case study: Jak zwykły spam może prowadzić do poważnych konsekwencji. Spojrzenie okiem biegłego sądowego z zakresu przestępstw przy pomocy systemów IT.
9. Zarządzanie aktywami informacyjnym.
10. Proces autoryzacji urządzeń mobilnych.

11. Analiza wykorzystania sprzętu prywatnego do celów służbowych. Analiza modeli BYOD (bring your own device), COPE (corporate owned personal enable), CYOD (choose your own device).
12. Najlepsze praktyki w zakresie cyberbezpieczeństwa stosowane na świecie:

- Zarządzanie dostępem do sieci i systemów IT.
- Korzystanie z sieci bezprzewodowych w pracy i w domu.
- Praca zdalna - ocena z perspektywy audytora. Ryzyka, rekomendacje.
- Zarządzanie hasłami;
- Wdrażania silnych mechanizmów ochrony przed kradzieżą sprzętu i tożsamości oraz nieautoryzowanym dostępem do zasobów organizacji.
- Dostęp uprzywilejowany,
- Polityka czystego biurka i czystego ekranu,
- Korzystanie z urządzeń końcowych nagrywających dźwięk i obraz.

13. Case study : Jak monitorować informatyków.
14. Case study : Mamy incydent i co teraz. Tworzenie schematu postępowania zarządzania incydentami.
15. Rola pracownika w doskonaleniu ochrony oraz postępowanie z najczęstszymi incydentami związanymi z bezpieczeństwem informacji.
16. Najczęstsze problemy zidentyfikowane w trakcie odbytych audytów z zakresu bezpieczeństwa.

Wymagania trenera: osoba prowadząca szkolenie powinna posiadać ważne na dzień realizacji szkolenia certyfikaty:

1. Audytor wiodący ISO/IEC 27001:2022 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności
2. Audytor wiodący ISO/IEC 27701 - System Zarządzania Informacjami o Prywatności
3. Audytor wiodący ISO/IEC 27018 – Kodeks postępowania w zakresie ochrony informacji umożliwiających identyfikację osoby w chmurach publicznych działających jako podmioty przetwarzające PII

3) SZKOLENIE DLA Administratorów

Szkolenia dla pracowników Urzędu Miasta Łomża w zakresie bezpieczeństwa informacji mają obejmować odpowiednio:
a) Szkolenie z zakresu bezpieczeństwa informacji w Urzędzie Miasta Łomży zostanie przeprowadzone w formie stacjonarnej w siedzibie Zamawiającego dla **8 uczestników**
b) Jednostką czasową szkolenia jest 1 godzina szkoleniowa (45 minut).
c) Szkolenia będą trwały minimum 16 godzin (2 dni)
d) Szkolenia będą odbywać się w dni robocze w godzinach 8.00 – 16.00.
e) Szkolenia będą prowadzone w języku polskim.
f) Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego harmonogramu zawierającego zakres merytoryczny, dostarczonego przez Wykonawcę Zamawiającemu przed podpisaniem umowy.

Szczegółowy opis przedmiotu zamówienia:
Organizacja i przeprowadzenie szkolenia:

Tematyka szkolenia będzie dotyczyła w szczególności następujących zagadnień z zakresu bezpieczeństwa informacji:

Dzień 1

1. Wprowadzenie do tematyki związanej z ochroną przed cyberzagrożeniami. Bezpieczeństwo informacji w świetle rozwijających się technologii
2. System zarządzania bezpieczeństwem informacji wynikających z ISO/IEC 27001, a cyberbezpieczeństwo. Kluczowe obszary.
3. Przegląd zagrożeń dla bezpieczeństwa informacji przetwarzanych formą tradycyjną oraz elektroniczną.
4. Źródła zagrożeń związanych z bezpieczeństwem informacji oraz ich klasyfikacja w oparciu o możliwe zdarzenia i straty dla organizacji.

5. Zarządzanie ryzykiem, jako kluczowy element ochrony. Podejście praktyczne.

6. Najczęstsze praktyki i sposoby wyłudzania, oszustw lub kradzieży informacji z organizacji:
   - wykradanie danych,
   - phishing i zaawansowane techniki wykorzystywane przez cyberprzestępców,
   - ataki socjotechniczne,
   - malware,
   - kontrola dostępu,
   - działania pracowników wewnętrznych na szkodę organizacji
   - techniki manipulacji,
   - biały wywiad,
   - ataki destrukcyjne.

7. Case study: atak ukierunkowany (APT) na osoby mające dostęp do systemów i danych finansowych.

8. Normy, standardy, wytyczne wspomagające zarządzanie systemami IT
   - ISO 2700x,
   - Krajowe Ramy Interoperacyjności,
   - RODO
   - Ustawa krajowy system cyberbezpieczeństwa,

Dzień 2

1. System Zarządzania bezpieczeństwem informacji.
2. Najlepsze praktyki zabezpieczania systemów informacyjnych.
3. Audyt teleinformatyczny krok po kroku…
   - infrastruktura IT i ochrona danych w data center/serwerowni,
   - podstawowa dokumentacja i wdrożone polityki bezpieczeństwa,
   - organizacji bezpieczeństwa informacji,
   - zarządzania aktywami IT,
   - kontrola dostępu (sieć, systemy, aplikacje, urządzenia)

- bezpieczeństwo sprzętu,
- zarządzania systemami i sieciami
- procedury eksploatacyjne i zakresy odpowiedzialności,
- zarządzanie usługami dostarczanymi przez strony trzecie,
- planowanie i odbiór systemów,
- ochrona przed kodem złośliwym,
- kopie zapasowe,
- zarządzanie bezpieczeństwem sieci,
- obsługa nośników,
- monitorowanie,
- bezpieczne sposoby wymiany informacji:
- przetwarzanie mobilne i praca na odległość,
- zarządzanie bezpieczeństwem danych przetwarzanych w modelu cloud,
- pozyskiwania i rozwoju systemów informatycznych,
- zarządzania relacjami z dostawcami,
- zarządzania incydentami w systemach IT,
- zarządzania ciągłością działania,
- compliance.

4. Najczęściej zidentyfikowane w czasie audytów czy kontroli incydenty, słabości, naruszenia i przestępstwa omówione z perspektywy audytora wiodącego i biegłego sądowego.

Wymagania trenera : osoba prowadząca szkolenie powinna posiadać ważne na dzień realizacji szkolenia certyfikaty:

1. Audytor wiodący ISO/IEC 27001:2022 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności
2. Audytor wiodący ISO/IEC 27701 - System Zarządzania Informacjami o Prywatności
3. Audytor wiodący ISO/IEC 27018 – Kodeks postępowania w zakresie ochrony informacji umożliwiających identyfikację osoby w chmurach publicznych działających jako podmioty przetwarzające PII