Szkolenie z cyberbezpieczeństwa dla pracowników biurowych

1. Przedmiot zamówienia

Przedmiotem zamówienia jest przygotowanie i przeprowadzenie **stacjonarnego szkolenia z zakresu cyberbezpieczeństwa dla pracowników biurowych** Zamawiającego, w wymiarze **od 6 do 8 godzin dydaktycznych**, dla grupy **do 20 uczestników**, wraz z opracowaniem i przeprowadzeniem **testów świadomości bezpieczeństwa** oraz przekazaniem materiałów szkoleniowych i dokumentacji potwierdzającej realizację usługi.

Szkolenie ma być ukierunkowane na podniesienie świadomości uczestników w zakresie zagrożeń cyberbezpieczeństwa, bezpiecznego korzystania z poczty elektronicznej, systemów informatycznych, Internetu, dokumentów oraz danych przetwarzanych w organizacji.

2. Cel zamówienia

Celem zamówienia jest:

1. podniesienie poziomu świadomości pracowników biurowych w zakresie cyberzagrożeń;
2. ograniczenie ryzyka incydentów bezpieczeństwa wynikających z błędów ludzkich;
3. przekazanie uczestnikom praktycznej wiedzy dotyczącej bezpiecznego korzystania z narzędzi informatycznych i informacji;
4. wykształcenie prawidłowych nawyków związanych z ochroną danych, dokumentów i systemów;
5. zwiększenie zdolności pracowników do rozpoznawania prób oszustw, phishingu, socjotechniki oraz innych typowych zagrożeń;
6. zwiększenie gotowości organizacji do zapobiegania incydentom oraz ich właściwego zgłaszania.

3. Grupa docelowa

1. Szkolenie przeznaczone jest dla **pracowników biurowych i administracyjnych** Zamawiającego oraz innych użytkowników systemów informatycznych, którzy nie pełnią funkcji technicznych w obszarze IT.
2. Liczba uczestników szkolenia wynosi **do 20 osób**.
3. Poziom szkolenia musi być dostosowany do odbiorców nietechnicznych, wykonujących codzienne obowiązki administracyjne, kancelaryjne, organizacyjne lub wspierające.

4. Forma i czas realizacji

1. Szkolenie musi zostać przeprowadzone **w formie stacjonarnej** w miejscu wskazanym przez Zamawiającego.
2. Łączny czas trwania szkolenia musi wynosić **od 6 do 8 godzin dydaktycznych**.
3. Szkolenie powinno zostać zrealizowane w ciągu **jednego dnia szkoleniowego**, chyba że Zamawiający wskaże inny podział czasowy.
4. Wykonawca zobowiązany jest zapewnić prowadzenie szkolenia w sposób uporządkowany, praktyczny i angażujący uczestników.

5. Zakres merytoryczny szkolenia

Szkolenie musi obejmować co najmniej następujące zagadnienia:

5.1. Wprowadzenie do cyberbezpieczeństwa

1. znaczenie cyberbezpieczeństwa w codziennej pracy biurowej;
2. rola pracownika w systemie bezpieczeństwa informacji;
3. najczęstsze przyczyny incydentów związanych z czynnikiem ludzkim.

5.2. Zagrożenia w poczcie elektronicznej i Internecie

1. phishing, spear phishing, smishing i inne formy wyłudzeń;
2. rozpoznawanie podejrzanych wiadomości, linków, załączników i domen;
3. fałszywe wiadomości od kontrahentów, przełożonych, urzędów, banków i dostawców;
4. podstawowe zasady bezpiecznego korzystania z Internetu i przeglądarki.

5.3. Socjotechnika i manipulacja

1. najczęstsze metody wpływu stosowane wobec pracowników;
2. wyłudzanie informacji przez telefon, e-mail, komunikatory i bezpośredni kontakt;

3. zasady weryfikacji nietypowych poleceń, próśb o dane, dostęp lub wykonanie operacji.

5.4. Hasła i bezpieczne logowanie

1. zasady tworzenia i stosowania silnych haseł;
2. najczęstsze błędy użytkowników w zakresie haseł;
3. uwierzytelnianie wieloskładnikowe i jego znaczenie;
4. bezpieczne przechowywanie danych uwierzytelniających.

5.5. Bezpieczna praca na stanowisku biurowym

1. korzystanie z komputera służbowego zgodnie z zasadami bezpieczeństwa;
2. blokowanie ekranu, wylogowywanie się, ochrona sesji użytkownika;
3. ryzyka związane z korzystaniem z nieautoryzowanych nośników i oprogramowania;
4. zagrożenia wynikające z nieuwagi, pośpiechu i rutyny.

5.6. Ochrona informacji i danych

1. bezpieczne przetwarzanie informacji służbowych i danych osobowych;
2. zasady ograniczonego dostępu do informacji;
3. bezpieczne udostępnianie, przesyłanie i przechowywanie dokumentów;
4. ochrona dokumentów papierowych oraz informacji wyświetlanych na ekranie.

5.7. Praca poza biurem i urządzenia mobilne

1. bezpieczne korzystanie z laptopów, telefonów i nośników danych;
2. podstawowe zasady bezpieczeństwa podczas pracy zdalnej i poza siedzibą organizacji;
3. ryzyka związane z publicznymi sieciami, podróżami i pracą w miejscach ogólnodostępnych.

5.8. Malware, ransomware i inne zagrożenia techniczne

1. podstawowe rodzaje złośliwego oprogramowania;
2. typowe sposoby infekcji urządzeń użytkowników;
3. sygnały ostrzegawcze mogące wskazywać na incydent;
4. podstawowe zasady ograniczania skutków zagrożeń.

5.9. Reagowanie na incydenty

1. czym jest zdarzenie i incydent bezpieczeństwa;
2. jak rozpoznać sytuację wymagającą reakcji;
3. jak i komu zgłaszać incydenty;
4. jakich działań użytkownik nie powinien podejmować samodzielnie.

5.10. Dobre praktyki bezpieczeństwa

1. codzienne zasady bezpiecznej pracy z informacją;
2. najczęstsze błędy użytkowników i sposoby ich unikania;
3. odpowiedzialność pracownika za bezpieczeństwo informacji w organizacji.

6. Sposób realizacji szkolenia

1. Szkolenie musi mieć charakter **praktyczny**, zorientowany na rzeczywiste sytuacje występujące w pracy biurowej.
2. Wykonawca zobowiązany jest uwzględnić przykłady, scenariusze, case study oraz omówienie typowych błędów użytkowników.
3. Szkolenie powinno być prowadzone językiem zrozumiałym dla osób nietechnicznych.
4. W trakcie szkolenia należy przewidzieć możliwość zadawania pytań przez uczestników.
5. Szkolenie powinno zawierać elementy angażujące uczestników, w szczególności:
    1. analizę przykładowych wiadomości phishingowych,
    2. omówienie sytuacji problemowych,
    3. krótkie ćwiczenia lub zadania praktyczne,
    4. dyskusję nad przykładami zdarzeń z codziennej pracy.

7. Testy świadomości bezpieczeństwa

1. W ramach realizacji zamówienia Wykonawca zobowiązany jest przygotować i przeprowadzić:
    1. **test wstępny** badający poziom świadomości uczestników przed szkoleniem;
    2. **test końcowy** badający poziom wiedzy i świadomości po zakończeniu szkolenia.
2. Testy muszą być dostosowane do zakresu szkolenia oraz poziomu uczestników.

3. Testy powinny obejmować zagadnienia praktyczne związane z codzienną pracą biurową, w szczególności rozpoznawanie zagrożeń, właściwe reakcje oraz podstawowe zasady bezpieczeństwa.
4. Wykonawca zobowiązany jest opracować wyniki testów w formie zbiorczego zestawienia lub krótkiego raportu, zawierającego co najmniej:
    1. liczbę uczestników,
    2. średni wynik testu wstępnego,
    3. średni wynik testu końcowego,
    4. ogólną ocenę poziomu świadomości uczestników,
    5. wnioski i rekomendacje dotyczące dalszych działań podnoszących świadomość.
5. Zamawiający dopuszcza przeprowadzenie testów w formie papierowej albo elektronicznej.

8. Materiały szkoleniowe

1. Wykonawca zobowiązany jest przygotować i przekazać uczestnikom materiały szkoleniowe w formie elektronicznej, a na żądanie Zamawiającego również w formie papierowej.
2. Materiały szkoleniowe muszą obejmować co najmniej:
    1. program szkolenia;
    2. prezentację lub opracowanie omawianych zagadnień;
    3. zestaw podstawowych zasad cyberbezpieczeństwa dla pracownika biurowego;
    4. przykłady zagrożeń i zalecanych reakcji;
    5. krótkie materiały utrwalające wiedzę po szkoleniu.
3. Materiały muszą być przygotowane w sposób czytelny, praktyczny i możliwy do wykorzystania po zakończeniu szkolenia.

9. Obowiązki Wykonawcy

Do obowiązków Wykonawcy należy w szczególności:

1. opracowanie programu szkolenia zgodnego z OPZ;
2. przygotowanie materiałów szkoleniowych;
3. przeprowadzenie szkolenia w formie stacjonarnej;
4. przygotowanie i przeprowadzenie testu wstępnego i końcowego;
5. zapewnienie trenera posiadającego odpowiednie kompetencje merytoryczne i dydaktyczne;
6. przeprowadzenie szkolenia w sposób dostosowany do grupy uczestników;
7. przekazanie Zamawiającemu materiałów szkoleniowych oraz wyników testów świadomości;
8. sporządzenie listy obecności uczestników;
9. wydanie uczestnikom zaświadczeń lub certyfikatów uczestnictwa, jeżeli Zamawiający tego wymaga.

10. Wymagania wobec Wykonawcy

1. Wykonawca musi posiadać **co najmniej 2-letnie doświadczenie** w realizacji szkoleń z zakresu cyberbezpieczeństwa, bezpieczeństwa informacji lub podnoszenia świadomości użytkowników w obszarze zagrożeń cyfrowych.
2. Osoba prowadząca szkolenie musi posiadać **co najmniej 2-letnie doświadczenie** w prowadzeniu szkoleń, warsztatów lub działań edukacyjnych z zakresu cyberbezpieczeństwa, bezpieczeństwa informacji lub ochrony danych dla użytkowników nietechnicznych, w szczególności pracowników administracyjnych lub biurowych.
3. Wykonawca zobowiązany jest zapewnić prowadzącego posiadającego wiedzę praktyczną oraz umiejętność przekazywania treści w sposób zrozumiały dla odbiorców nietechnicznych.
4. Na żądanie Zamawiającego Wykonawca przedstawi wykaz zrealizowanych usług lub inne dokumenty potwierdzające spełnienie wymagań dotyczących doświadczenia.

11. Dokumentacja i rezultaty realizacji

Po zakończeniu szkolenia Wykonawca przekaże Zamawiającemu:

1. program szkolenia;
2. materiały szkoleniowe;
3. listę obecności;
4. wzór testu wstępnego i końcowego albo ich treść;

5. zestawienie wyników testów świadomości;
6. certyfikaty dla uczestników

Obowiązki Zamawiającego do wszystkich szkoleń

- rekrutacja uczestników na szkolenia
- udostepnienie sal szkoleniowych
- dostosowanie wymogów szkoleń do potrzeb OzN
- przeprowadzenie ankiety specjalnych potrzeb wśród uczestników szkoleń