

## OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ) – Część 4

na realizację zamówienia: **Szkolenia specjalistyczne w zakresie „Security Awareness – jak być świadomym użytkownikiem”** w ramach projektu pn. „Cyberbezpieczny Samorząd”

### Rozdział I – PRZEDMIOT ZAMÓWIENIA

Przedmiotem zamówienia jest świadczenie usługi polegającej na zorganizowaniu i przeprowadzeniu specjalistycznych szkoleń dla uczestników zgodnie z poniższym zestawieniem:

Lp.	Temat szkolenia	Liczba uczestników	Uczestnicy
1	Security Awareness – jak być świadomym użytkownikiem	50	pracownicy urzędu

Szkolenia mogą być realizowane w trybie:

- **online w sali narad Urzędu Miejskiego,**
- **online** (z wykorzystaniem platformy szkoleniowej zapewnionej przez Wykonawcę lub Zamawiającego).

### Rozdział II – CEL SZKOLENIA

Celem szkolenia jest nabycie przez uczestników wiedzy i umiejętności w zakresie:

- rozpoznawania najczęściej występujących zagrożeń cyberbezpieczeństwa,
- bezpiecznego korzystania z systemów informatycznych, Internetu i poczty elektronicznej,
- stosowania zasad cyberhigieny w codziennej pracy,
- właściwego reagowania na incydenty bezpieczeństwa,
- ograniczania ryzyka wynikającego z manipulacji socjotechnicznych, phishingu oraz innych form oszustw,
- ochrony danych osobowych i informacji przetwarzanych w urzędzie,
- budowania świadomych i bezpiecznych nawyków cyfrowych w środowisku pracy i poza nim.

Szkolenie ma na celu podniesienie poziomu bezpieczeństwa informacyjnego urzędu poprzez zwiększenie świadomości pracowników oraz ich odporności na działania cyberprzestępców.

### Rozdział III – ZAKRES SZKOLENIA

Zakres szkolenia obejmuje przekazanie wiedzy teoretycznej oraz praktycznych umiejętności w obszarze bezpieczeństwa cyfrowego, w szczególności:

#### 1. Wprowadzenie do cyberbezpieczeństwa

- podstawowe pojęcia i zagrożenia,
- rola użytkownika w systemie bezpieczeństwa urzędu,

- przykłady incydentów i ich konsekwencje dla administracji publicznej.

## 2. Cyberhigiena

- zasady tworzenia i przechowywania haseł,
- stosowanie uwierzytelniania wieloskładnikowego,
- aktualizacje oprogramowania i bezpieczne korzystanie z urządzeń,
- zasady pracy zdalnej i mobilnej.

## 3. Phishing i socjotechnika

- rozpoznawanie prób wyłudzenia danych,
- analiza fałszywych wiadomości e-mail, SMS i komunikatów,
- techniki manipulacji stosowane przez cyberprzestępców,
- właściwe reakcje na podejrzane wiadomości.

## 4. Bezpieczne korzystanie z Internetu i poczty elektronicznej

- identyfikacja fałszywych stron logowania,
- ryzyka związane z pobieraniem plików,
- ochrona przed malware i ransomware,
- zasady bezpiecznej komunikacji elektronicznej.

## 5. Ochrona danych i prywatności

- dane osobowe i dane wrażliwe – podstawy,
- zasady czystego biurka i czystego ekranu,
- bezpieczne przechowywanie i przesyłanie informacji,
- praca na danych urzędowych poza biurem.

## 6. Media społecznościowe

- zagrożenia wynikające z nadmiernego ujawniania informacji,
- bezpieczne ustawienia prywatności,
- oszustwa i manipulacje w social media.

## 7. Bezpieczeństwo urządzeń i sieci

- bezpieczne korzystanie z sieci Wi-Fi (domowej i publicznej),
- stosowanie VPN,

- szyfrowanie danych,
- zagrożenia związane z urządzeniami IoT.

## 8. Reagowanie na incydenty

- rozpoznawanie symptomów ataku,
- procedury zgłaszania incydentów w urzędzie,
- działania minimalizujące skutki incydentu,
- czego unikać w sytuacji zagrożenia.

## 9. Najlepsze praktyki bezpieczeństwa

- codzienne dobre nawyki użytkownika,
- checklisty bezpieczeństwa,
- przykładowe scenariusze i właściwe reakcje.

## 10. Elementy praktyczne (opcjonalnie)

- analiza przykładowych ataków phishingowych,
- rozpoznawanie fałszywych stron logowania,
- symulacje socjotechniczne,
- test wiedzy końcowej.

## Rozdział IV – WYMAGANIA WOBEC WYKONAWCY

Wykonawca zobowiązany jest do:

1. zapewnienia trenera posiadającego:
  - minimum **2 lata doświadczenia** w prowadzeniu szkoleń z zakresu cyberbezpieczeństwa,
  - wiedzę praktyczną potwierdzoną realizacją podobnych szkoleń,
  - umiejętność prowadzenia zajęć w sposób interaktywny i zrozumiały dla użytkowników nietechnicznych;
2. przygotowania i dostarczenia materiałów szkoleniowych w formie elektronicznej (PDF);
3. zapewnienia narzędzi i środowiska do realizacji szkolenia online (jeśli szkolenie odbywa się na platformie Wykonawcy);
4. przeprowadzenia szkolenia zgodnie z programem zaakceptowanym przez Zamawiającego;
5. przygotowania i przeprowadzenia ankiety ewaluacyjnej;
6. opracowania raportu końcowego zawierającego:

- podsumowanie przebiegu szkolenia,
- wyniki ankiet,
- rekomendacje dotyczące dalszych działań podnoszących bezpieczeństwo.

## **Rozdział V – WYMAGANIA ORGANIZACYJNE**

### **1. Po stronie Wykonawcy**

- zapewnienie prowadzącego szkolenie,
- dostarczenie materiałów szkoleniowych,
- przygotowanie certyfikatów ukończenia szkolenia,
- zapewnienie narzędzi do realizacji szkolenia online (jeśli dotyczy),
- przygotowanie ankiet i raportu końcowego.

### **2. Po stronie Zamawiającego**

- udostępnienie sali narad Urzędu Miejskiego (w przypadku szkolenia online realizowanego lokalnie),
- zapewnienie sprzętu multimedialnego (projektor, ekran, nagłośnienie),
- zapewnienie dostępu do Internetu,
- wskazanie osoby odpowiedzialnej za kontakt z Wykonawcą.

## **Rozdział VI – REZULTATY SZKOLENIA**

Po zakończeniu szkolenia uczestnicy powinni:

- rozpoznawać najczęstsze zagrożenia cyberbezpieczeństwa,
- stosować zasady cyberhigieny w codziennej pracy,
- bezpiecznie korzystać z poczty elektronicznej i Internetu,
- właściwie reagować na podejrzane wiadomości i incydenty,
- chronić dane osobowe i informacje urzędowe,
- unikać zachowań zwiększających ryzyko naruszenia bezpieczeństwa.

## **Rozdział VII – KRYTERIA ODBIORU**

Szkolenie zostanie uznane za wykonane prawidłowo, jeśli:

1. zostanie przeprowadzone zgodnie z programem i harmonogramem,
2. Wykonawca dostarczy materiały szkoleniowe i certyfikaty,
3. zostaną przeprowadzone ankiety ewaluacyjne,



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA

4. co najmniej **80% uczestników** oceni szkolenie pozytywnie,
5. Wykonawca dostarczy raport końcowy w wymaganym terminie.

## Rozdział VIII – HARMONOGRAM

- Szkolenia ma się odbyć w dwóch grupach w dwóch różnych terminach w dni robocze ustalone wcześniej z Zamawiającym
- Zajęcia odbywają się w godzinach 9:00–13:00.
- Termin przekazania materiałów szkoleniowych: **najpóźniej 3 dni przed szkoleniem**
- Termin przekazania raportu końcowego: **do 7 dni po zakończeniu szkolenia**