

Załącznik nr 1 do zapytania ofertowego

Opis przedmiotu zamówienia

I. Zamówienie obejmuje Przeprowadzenie szkolenia pracowników Urzędu Gminy i jednostek podległych z zakresu cyberbezpieczeństwa

II. Liczba jednostek objętych zamówieniem 3 jednostki (Urząd oraz 2 podległe JST):

- Urząd Gminy Bodzechów z/s w Ostrowcu Św.
- Gminny Ośrodek Pomocy Społecznej w Bodzechowie z/s w Ostrowcu Św.
- Gminne Centrum Oświaty w Bodzechowie

III. Liczba osób objętych szkoleniem:

- Urząd Gminy Bodzechów z/s w Ostrowcu Św. – łącznie **45** osób
- Gminny Ośrodek Pomocy Społecznej w Bodzechowie z/s w Ostrowcu Św. – **10** osób
- Gminne Centrum Oświaty w Bodzechowie – **5** osób

IV. Opis przedmiotu zamówienia:

1. Wykonawca jest zobowiązany do przeprowadzenia szkolenia pracowników **Urzędu Gminy i jednostek podległych** z zakresu cyberbezpieczeństwa **dedykowanego dla JST** w terminie od podpisania umowy do **25.05.2026 r.**

2. Wykonawca musi wykazać, że:

- w okresie od **01.01.2023 r.** do **28.04.2026 r.** wykonał **należycie co najmniej 4** zamówienia obejmujące wykonanie szkoleń z zakresu cyberbezpieczeństwa w jednostkach sektora finansów publicznych z zastrzeżeniem minimum po jednym w **2026, 2025, 2024 i 2023** roku. (Wymagamy uzupełnienia **Załącznika nr 4 – Wykaz usług** a także dołączenia dokumentów potwierdzających wykonanie usługi np. **referencji**),
- trener który będzie realizował zamówienie przeprowadził w okresie od **01.01.2023 r.** do **28.04.2026 r.** wykonał **przynajmniej 4** szkolenia na temat cyberbezpieczeństwa w jednostkach sektora finansów publicznych z zastrzeżeniem minimum po jednym w **2026, 2025, 2024 i 2023** roku. (Wymagamy uzupełnienia **Załącznika nr 5 – Wykaz osób** a także dołączenia dokumentu potwierdzającego posiadane kwalifikacje np. **certyfikat**),

- gwarantuje wysoką jakość usług szkoleniowych w związku z posiadaniem certyfikatu systemu zarządzania jakością zgodnego z normą PN-EN ISO 9001:2015-10.

3. Program szkolenia powinien obejmować minimum poniższy zakres tematyczny:

- 1) Główne założenia i wymagania prawne cyberbezpieczeństwa w pracy urzędnika.
- 2) System Zarządzania Bezpieczeństwem Informacji – cele jego funkcjonowania.
- 3) Rodzaje incydentów bezpieczeństwa i zasady postępowania z incydemem.
- 4) Omówienie przykładowych ataków: ataki socjotechniczne, ataki komputerowe, ataki przez sieci bezprzewodowe, ataki przez pocztę e-mail (fałszywe e-maile, weryfikacja odbiorcy i nadawcy), ataki przez strony www, ataki przez telefon, phishing, spoofing, spam.
- 5) Bezpieczeństwo fizyczne – urządzenia, dokumenty, „czyste biurko”, „czysty ekran”, klucze do pomieszczeń.
- 6) Zabezpieczenia informatyczne nośników danych – pendrive i dyski zewnętrzne (demonstracja szyfrowania pendrive).
- 7) Zdalny dostęp do zasobów jednostki i korzystanie z urządzeń prywatnych przez pracowników oraz związane z tym potencjalne zagrożenia.
- 8) Monitorowanie i korzystanie z oprogramowania antywirusowego (demonstracja skanowania pendrive, nośnika zewnętrznego).
- 9) Zasady bezpiecznego korzystania z systemu operacyjnego Windows.
- 10) Szyfrowanie plików i poczty elektronicznej (demonstracja).
- 11) Polityka haseł, zarządzanie dostępem i tożsamością.
- 12) Sposoby tworzenia backupu, kopii bezpieczeństwa. Retencja i archiwizacja danych
- 13) Niebezpieczeństwo związane z chatbotami AI, ryzyko nadmiernego udostępniania.
- 14) Jak bezpiecznie korzystać z chatbotów AI?
- 15) Sesja pytań i odpowiedzi.

4. Wymagania ogólne dotyczące organizacji szkolenia:

- 1) Szkolenie odbędzie się w siedzibie Zamawiającego, w trybie stacjonarnym. Nie dopuszcza się możliwości realizacji usługi za pomocą środków zdalnej komunikacji.

2) Zamawiający udostępni salę, projektor multimedialny i dostęp do Internetu – wykonawca dostarczy laptopa i wszystkie niezbędne materiały.

3) W szkoleniu będzie brało udział **60 osób, w podziale na 6 grup (6 grup po 10 osób)**. Zamawiający dopuszcza rotacje w liczbie uczestników podczas każdego szkolenia. Wymagane jest aby każda grupa miała szkolenie w innym terminie. Szkolenie ma być prowadzone jednocześnie tylko dla jednej grupy. Maksymalnie mogą zostać przeszkolone 3 grupy w ciągu jednego dnia. Szkolenia będą odbywać się w dni robocze, w godz. 7:00 – 15:00. Szkolenie będzie prowadzone w języku polskim. Czas szkolenia 3 godziny lekcyjne po 45 minut. Szczegółowa data szkolenia będzie ustalana z Zamawiającym. **Każdy Uczestnik szkolenia otrzyma materiały szkoleniowe w języku polskim na pendrive, certyfikat ukończenia szkolenia oraz dostęp do platformy e-learningowej do 30 czerwca 2026 r. Platforma ma dostarczyć zasoby i materiały niezbędne do zapewnienia pracownikom wartościowej wiedzy i umiejętności w zakresie ochrony przed cyberzagrożeniami. W ramach dostarczonej platformy użytkownicy muszą otrzymać dostęp do materiałów szkoleniowych oraz testów wiedzy w języku polskim.**

4) Wykonawca zobowiązuje się w terminie 7 dni od podpisania umowy dostarczyć Zamawiającemu:

- a) Proponowany zakres tematyczny,
- b) Dzienny harmonogram szkolenia.

Wykonawca zobowiązany jest do współpracy i konsultacji z Zamawiającym oraz do wprowadzania poprawek w sporządzanej przez siebie dokumentacji szkoleniowej zgodnie z sugestiami Zamawiającego na każdym etapie realizacji zamówienia. Szkolenia mogą zostać przeprowadzone po akceptacji dokumentacji przez Zamawiającego.

5) W ramach organizacji szkolenia Wykonawca zapewni:

1. Materiały szkoleniowe, obejmujące szczegółowy zakres merytoryczny szkolenia i harmonogram dzienny szkolenia.
2. Właściwe działania promocyjne i informacyjne dotyczące szkoleń, w tym oznakowanie w odpowiedni sposób materiałów szkoleniowych przekazanych uczestnikowi. Zasady zostały określone w Podręczniku wnioskodawcy i beneficjenta Funduszy europejskich na lata 2021-2027 w zakresie informacji i promocji opublikowanym na stronie internetowej www.funduszeuropejskie.gov.pl
3. Wydanie uczestnikowi szkolenia zaświadczenia/certyfikatu o ukończeniu szkolenia.
4. Kadrę trenerską posiadającą wiedzę, doświadczenie i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkolenia.
5. Prowadzenie dokumentacji wszystkich szkoleń w jednakowy sposób. Na dokumentację szkolenia składa się:
 - a) Lista obecności uczestnika
 - b) Sporządzony przez trenera dziennik szkolenia, zawierający szczegółowe informacje na temat przebiegu oraz zakresu merytorycznego szkolenia, podpisany po zakończeniu szkolenia

przez prowadzącego szkolenie.

Wykonawca zobowiązany jest do przekazania dokumentacji szkolenia w formie papierowej.

6. Wykonawca ma obowiązek przestrzegania zasad równościowych podczas realizacji zamówienia, ze szczególnym uwzględnieniem przekazu równych szans kobiet i mężczyzn, informowania uczestników zajęć o współfinansowaniu projektu ze środków Unii Europejskiej,

6) Wykonawca zobowiązany jest do pokrycia wszystkich kosztów związanych z wykonaniem przedmiotu zamówienia w tym materiałów szkoleniowych, zaświadczeń czy certyfikatów.