

Załącznik Nr 2 do Rozeznania rynku

OPIS PRZEDMIOTU ZAMÓWIENIA

Przeprowadzenie szkoleń z podstaw cyberbezpieczeństwa dla pracowników administracyjnych oraz szkoleń dla kadry kierowniczej w ramach projektu pn.: „Zwiększenie poziomu cyberbezpieczeństwa Powiatu Ostrowieckiego”

1. Przedmiotem zamówienia jest przeprowadzenie szkoleń z podstaw cyberbezpieczeństwa dla pracowników administracyjnych Starostwa Powiatowego, Powiatowego Urzędu Pracy i Powiatowego Centrum Pomocy Rodzinie oraz szkoleń dla kadry kierowniczej ww. jednostek, w zakresie dotyczącym bezpieczeństwa informacji, a także zagadnień związanych z identyfikacją zagrożeń, zarządzaniem ryzykiem oraz zarządzaniem incydentami.
2. Celem szkoleń jest zapewnienie skutecznego i dostosowanego do potrzeb jednostek przekazania wiedzy, umiejętności oraz praktycznych narzędzi związanych z ochroną przed zagrożeniami w cyberprzestrzeni, jak również z wdrażaniem i utrzymywaniem Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).
3. Ilość szkoleń oraz termin realizacji/wykonania zamówienia:
 - 1) **szkolenia dla pracowników administracyjnych:**
 - Starostwa Powiatowego i Powiatowego Centrum Pomocy Rodzinie – **2 szkolenia**, w tym **drugie szkolenie jako przypominające**
 - Powiatowego Urzędu Pracy – **1 szkolenie**,
 - 2) **szkolenia dla kadry kierowniczej:**
 - Starostwa Powiatowego – **2 szkolenia**, w tym **drugie szkolenie jako przypominające**
 - Powiatowego Centrum Pomocy Rodzinie i Powiatowego Urzędu Pracy – **1 szkolenie**,przy czym:
 - **pierwsze szkolenie – w terminie do dnia 31.10.2025 r.**
 - **drugie szkolenie (przypominające) – w terminie do dnia 31.03.2026 r.**

Konkretne terminy szkoleń Wykonawca ustali z Zamawiającym po podpisaniu umowy.
4. Liczba pracowników objętych szkoleniami: **łącznie 232 osoby**, z czego:
 - pracownicy administracyjni – **193 osoby**
 - kadra kierownicza - **39 osób**
 - 1) W rozbiciu na poszczególne jednostki:
 - Starostwo Powiatowe: łącznie **130 osób**, z czego:
 - pracownicy administracyjni: **104 osoby**
 - kadra kierownicza: **26 osób**

- Powiatowy Urząd Pracy: łącznie **50 osób**, z czego:
 - pracownicy administracyjni: **46 osób**
 - kadra kierownicza: **4 osoby**
- Powiatowe Centrum Pomocy: łącznie **52 osoby**, z czego:
 - pracownicy administracyjni: **43 osoby**
 - kadra kierownicza: **9 osób**.

5. Wymagania odnośnie organizacji szkoleń:

- 1) Szkolenia będą prowadzone stacjonarnie w budynku Starostwa Powiatowego w Ostrowcu Świętokrzyskim.
- 2) Szkolenia będą odbywać się w dni robocze od pon. do pt. w godzinach 8.00 – 15.00.
- 3) Zamawiający udostępni salę, projektor multimedialny i dostęp do Internetu – wykonawca dostarczy laptopa i wszystkie niezbędne materiały.
- 4) Szkolenia będą prowadzone w języku polskim i przedstawione w sposób zrozumiały przez osoby nietechniczne.
- 5) Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego szczegółowego zakresu merytorycznego dostarczonego przez Wykonawcę po podpisaniu umowy.
- 6) Szkolenia prowadzone będą w formie wykładu przeplatane demonstracjami wraz z angażowaniem uczestników do udziału.
- 7) Szkolenia będą prowadzone w grupach dedykowanych dla poszczególnych jednostek objętych wsparciem.
- 8) Szkolenia dla pracowników z podstaw cyberbezpieczeństwa będą prowadzone w sesjach po **max. 40 osób**.
- 9) Szkolenia dla kadry kierowniczej będą prowadzone w sesjach po **max. 15 osób**.
- 10) Ostateczna ilość sesji szkoleń oraz liczba osób biorących udział w każdej sesji z uwzględnieniem jednostek objętych wsparciem zostanie ustalona po podpisaniu umowy pomiędzy Wykonawcą a Zamawiającym.
- 11) Przewidywany czas trwania szkolenia: ok. 4h dla pojedynczej sesji (z przerwami).
- 12) W przypadku szkoleń trwających do 3 godzin, przewiduje się jedną przerwę trwającą 15 minut. W przypadku szkoleń trwających powyżej 3 godzin, organizowane będą dwie przerwy trwające 15 minut każda.

6. Warunki udziału w postępowaniu:

W postępowaniu mogą wziąć udział Wykonawcy, którzy są zdolni do wykonywania przedmiotu zamówienia i spełniają warunki w zakresie:

- 1) posiadania niezbędnej wiedzy oraz doświadczenia w zakresie objętym zamówieniem,
- 2) dysponowania odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania przedmiotu zamówienia,
- 3) posiadania wiedzy i doświadczenia w wykonywaniu przedmiotu zamówienia. Wymagane jest, aby w ciągu ostatnich **3 lat** przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – to w tym okresie – **wykonał należycie co najmniej 3 usługi polegające na przeprowadzeniu szkoleń z zakresu cyberbezpieczeństwa, dedykowane dla jednostek samorządu terytorialnego.**

7. Zakres szkoleń powinien obejmować minimum poniższy zakres tematyczny:

1) **Szkolenie dla pracowników z podstaw cyberbezpieczeństwa**

Szkolenie mające na celu podniesienie świadomości pracowników administracyjnych Starostwa Powiatowego, Powiatowego Urzędu Pracy oraz Powiatowego Centrum Pomocy Rodzinie w zakresie bezpieczeństwa danych oraz cyberbezpieczeństwa. Uczestnik szkolenia powinien zdobyć wiedzę na temat najnowszych zagrożeń, technik i metod socjotechnicznych stosowanych podczas ataków, a także poznać wzory oraz procedury właściwego zachowania w trakcie oraz po wykryciu ataku, w tym znaczenie przestrzegania przyjętych w organizacji polityk i procedur. Uczestnicy szkolenia powinni pozyskać niezbędną wiedzę obejmującą bezpieczne zarządzanie miejscem pracy oraz danymi, a także umożliwiającą skuteczną ochronę przed atakami zarówno w miejscu pracy, jak i w życiu prywatnym. Szkolenie powinno być dostosowane do specyfiki środowiska, w którym pracują uczestnicy szkolenia oraz odnosić się do wytycznych obowiązujących w danej jednostce.

Minimalny zakres tematyczny szkolenia:

- Przegląd aktualnego ustawodawstwa w zakresie bezpieczeństwa danych oraz cyberbezpieczeństwa (Ustawa o Krajowym Systemie Cyberbezpieczeństwa, KRI, RODO oraz NIS2), w tym obowiązki i odpowiedzialność pracowników.
- Konsekwencje cyberataków dla organizacji oraz poszczególnych pracowników.
- Cele współczesnej cyberprzestępczości, w szczególności w odniesieniu do sektora administracji publicznej.
- Kanały wykorzystywane do prowadzenia cyberataków – email, strony www, komunikatory, telefon, itp.,
- Rodzaje ataków – ataki socjotechniczne, ransomware, APT, phishing, smishing, spear-phishing, pharming, spoofing, spam, spim, scam, deepfake, kradzież tożsamości, itp.
- Metody ochrony przed atakami komputerowymi i socjotechnicznymi.
- Bezpieczne korzystanie z sieci bezprzewodowych (Wi-Fi, Bluetooth).
- Bezpieczne korzystanie z urządzeń mobilnych (telefony, tablety, laptopy).
- Bezpieczne korzystanie z poczty elektronicznej i Internetu.
- Bezpieczna praca z oprogramowaniem biurowym.
- Polityka haseł – jakie hasło jest bezpieczne, jak nimi zarządzać?
- Metody szyfrowania dokumentów elektronicznych.
- Bezpiecznie przechowywanie i usuwanie danych na komputerze i pendrive.
- Bezpieczny zdalny dostęp do zasobów firmowych.
- Bezpieczne stanowisko pracy – zasada czystego biurka, blokowanie komputerów, metody zabezpieczania, przechowywania i niszczenia dokumentów papierowych, zamykanie pomieszczenia, itp.
- Bezpieczeństwo fizyczne i ochrona miejsca pracy.
- Rozpoznawanie i obsługa incydentów – wzorce zachowań i procedury zgodne z polityką bezpieczeństwa informacji w organizacji.

Szkolenie powinno zakończyć się testem wiedzy, wydaniem imiennego certyfikatu dla każdego uczestnika szkolenia oraz przekazaniem każdemu uczestnikowi szkolenia materiału w formie papierowej w postaci **Checklisty „Bezpieczny Pracownik”**
Podsumowanie zasad: 10 punktów do powieszenia przy biurku (np. „Zawsze blokuj komputer”, „Sprawdzaj nadawcę e-maili”).

2) Szkolenie dla kadry kierowniczej

Szkolenie mające na celu przygotowanie kadry kierowniczej Starostwa Powiatowego, Powiatowego Urzędu Pracy oraz Powiatowego Centrum Pomocy Rodzinie do wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji.

Uczestnicy szkolenia powinni pozyskać niezbędną wiedzę zarządczą w zakresie bezpieczeństwa informacji, systemu zarządzania bezpieczeństwem informacji, a także zagadnień związanych identyfikacją zagrożeń, zarządzaniem ryzykiem, podatnościami oraz incydentami.

Uczestnicy szkolenia powinni zdobyć wiedzę niezbędną do wdrożenia i utrzymywania Systemu Zarządzania Bezpieczeństwa Informacji w oparciu o wymagania zawarte w normach ISO 27001 oraz NIS2.

Minimalny zakres tematyczny szkolenia:

- Wymagania ustawowe obowiązujące Jednostki Samorządu Terytorialnego w zakresie ochrony bezpieczeństwa informacji: KRI, UoKSC, RODO i inne – ochrona danych osobowych, tajemnica przedsiębiorstwa, tajemnica zawodowa, ochrona informacji niejawnych, ochrona praw autorskich, obowiązki i odpowiedzialność kadry kierowniczej oraz pracowników.
- Podstawowe kryteria ochrony informacji – poufność, integralność, dostępność.
- Kultura organizacyjna ochrony informacji – świadomość, odpowiedzialność.
- Polityka organizacyjna, ochrony fizycznej, personalna.
- Podstawowa dokumentacja regulująca proces zarządzania bezpieczeństwem informacji w organizacji - kompleksowa Polityka Bezpieczeństwa Informacji.
- Elementy Systemu Zarządzania Bezpieczeństwem Informacji.
- Role w systemie zarządzania bezpieczeństwem informacji – IOD, ASI.
- Zarządzanie ryzykiem - analiza ryzyka jako podstawa wdrażania SZBI - identyfikacja oraz analiza ryzyka w obszarze bezpieczeństwa informacji i bezpieczeństwa IT.
- Zarządzanie incydentami.
- Proces wdrażania SZBI - planowanie, implementacja oraz nadzór nad pracami wdrożeniowymi.
- Nowelizacja ustawy o Krajowym Systemie Cyberbezpieczeństwa oraz dyrektywa NIS2: jakie obowiązki dla urzędów, różnice pomiędzy podmiotem publicznym ważnym a podmiotem publicznym kluczowym, system zarządzania bezpieczeństwem informacji, zgłaszanie incydentów.

Szkolenie powinno zakończyć się testem wiedzy, wydaniem imiennego certyfikatu dla każdego uczestnika szkolenia oraz przekazaniem każdemu uczestnikowi szkolenia materiału w formie papierowej w postaci **Checklisty „Bezpieczny Pracownik”** **Podsumowanie zasad: 10 punktów do powieszenia przy biurku** (np. „Zawsze blokuj komputer”, „Sprawdzaj nadawcę e-maili”).

8. Każdy blok szkoleniowy musi uwzględniać specyfikę grupy uczestników – inne materiały i metody pracy będą stosowane dla kadry kierowniczej, a inne dla pozostałych pracowników.
9. Szczegółowy zakres szkoleń zostanie uzgodniony z Zamawiającym po podpisaniu umowy. Wykonawca zobowiązany jest do przedstawienia Zamawiającemu konspektu szkoleń do zatwierdzenia.
10. 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.
11. Treść szkoleń powinien uwzględniać zagadnienia określone w normie ISO 27001 oraz NIS2.
12. Zakres szkoleń oraz tematyka powinny pokrywać się z treścią poradnika Ministerstwa Cyfryzacji oraz NASK p.t. „Cyberbezpieczny Samorząd” dostępnego na stronie <https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad>.
13. Tematyka szkoleń powinna uwzględniać wnioski oraz zalecenia Najwyższej Izby Kontroli p.t. „Zarządzanie bezpieczeństwem Informacji w jednostkach samorządu terytorialnego” z dn. 18.02.2019, Nr ewid.187/2018/P/18/006/KAP.
14. Wykonawca zobowiązany jest do pokrycia wszelkich kosztów związanych z wykonaniem przedmiotu zamówienia, w tym materiałów szkoleniowych oraz certyfikatów.
15. W ramach organizacji szkoleń Wykonawca zapewni:
 - 1) Właściwe działania promocyjne i informacyjne dotyczące szkoleń, w tym oznakowanie w odpowiedni sposób materiałów szkoleniowych przekazanych uczestnikom. 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
 - 2) Kadre trenerską posiadającą wiedzę, doświadczenie i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkolenia.
 - 3) Prowadzenie dokumentacji szkoleń, na którą składa się:
 - lista obecności uczestników;
 - sporządzony przez trenera dziennik szkolenia, zawierający szczegółowe informacje na temat przebiegu oraz zakresu merytorycznego szkolenia, podpisany po zakończeniu szkolenia przez prowadzącego szkolenie.

- materiały szkoleniowe dla uczestników, obejmujące szczegółowy zakres szkolenia, harmonogram dzienny szkolenia oraz materiały merytoryczne (np. skrypty, podręczniki, zeszyty informacyjne, broszury) w formie papierowej, zawierające szczegółowe informacje, które będą omawiane podczas szkolenia.
12. Wykonawca zobowiązany jest do przekazania dokumentacji ze szkolenia w formie papierowej.
 13. Wykonawca ma obowiązek przestrzegania zasad równościowych podczas realizacji zamówienia, ze szczególnym uwzględnieniem przekazu równych szans kobiet i mężczyzn i niedyskryminacji, w tym zapewnienie dostępności dla osób z niepełnosprawnościami oraz informowania uczestników zajęć o współfinansowaniu projektu ze środków Unii Europejskiej.
 14. Wykonawca zobowiązany jest do pokrycia wszystkich kosztów związanych z wykonaniem przedmiotu zamówienia w tym materiałów szkoleniowych oraz certyfikatów dla wszystkich uczestników szkoleń.