OR-3.271.1.2025 Załącznik nr 1 do zapytania ofertowego

# SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

***Zakup usług szkoleń stacjonarnych oraz e-learningowych z ochrony danych osobowych i cyberbezpieczeństwa w ramach projektu grantowego „Cyberbezpieczny samorząd”***

## I. Wstęp

Niniejszy dokument stanowi szczegółowy opis przedmiotu zamówienia na zakup usług szkoleń stacjonarnych oraz e-learningowych.

## II. Przedmiot zamówienia

Celem szkoleń jest podniesienie świadomości pracowników w zakresie ochrony danych oraz cyberbezpieczeństwa.

1. **<u>Część 1 – Usługa szkoleń stacjonarnych:</u>**

**Miejsce świadczenia usługi:** Urząd Gminy w Kościelcu, ul. Turecka 7/3, 62-604 Kościelec, woj. wielkopolskie, sala konferencyjna;

**Liczba uczestników:**

- Pracownicy biurowi Urzędu Gminy Kościelec 23 osoby
- Kadra zarządzająca Urzędu Gminy Kościelec 4 osoby

**Czas szkoleń**: Dla każdej grupy uczestników szkoleń w każdym z cyklów szkoleniowych z osobna zamawiający przewiduje ilość godzin szkolenia w wymiarze nie mniej niż 6 godzin.

**Planowane terminy szkoleń:** Zamawiający planuje 1 cykl szkoleniowy z podziałem na 2 grupy pracowników nie większe niż 15 osób w terminie kwiecień – maj 2025 r. Szczegółowy termin szkoleń zostanie uzgodniony z Wykonawcą najpóźniej na 3 dni robocze przed rozpoczęciem cyklu szkoleniowego.

Po podpisaniu umowy z Wykonawcą Zamawiający dopuszcza rotacje liczby uczestników podczas każdego cyklu szkoleniowego;

Szkolenia odbywać się będą w dni robocze od poniedziałku do czwartku w godzinach 7:30 – 15:30 oraz w piątki od godziny 7:30 do 14:30;

**Wymagania wobec Wykonawcy:**

- Wykonawca w ciągu ostatnich 3 lat przeprowadził minimum 4 szkolenia o tematyce cyberbezpieczeństwa i ochrony danych dla jednostek administracji publicznej lub państwowej;
- Wykonawca oddeleguje do realizacji zadania minimum jedną osobę, która posiada minimum 3-letnie doświadczenie w prowadzeniu szkoleń o tematyce cyberbezpieczeństwa;
- Wykonawca przeprowadzi szkolenia w języku polskim;
- Wykonawca wyda każdemu uczestnikowi szkolenia certyfikat o ukończeniu szkolenia (każdego z cykli szkolenia);

- W ramach organizacji każdego z cykli szkoleń stacjonarnych Wykonawca zapewni materiały szkoleniowe dla wszystkich uczestników obejmujące szczegółowy zakres merytoryczny w wersji papierowej. Materiały oraz wszystkie dokumenty muszą spełniać standardy dostępności oraz zostaną prawidłowo ologowane (oznaczone) zgodnie z Podręcznikiem wnioskodawcy i beneficjenta programów polityki spójności 2021-2027 w zakresie informacji i promocji;
- Wykonawca zobowiązuje się do przeprowadzenia cyklu szkoleń zgodnie z wytycznymi w zakresie realizacji zasad równości szans i niedyskryminacji, w tym dostępności dla osób z niepełnosprawnościami oraz zasady równości kobiet i mężczyzn w ramach Funduszy Unijnych na lata 2021-2027 zamieszczonymi na stronie www.funduszeeuropejskie.gov.pl w szczególności wytycznych dotyczących zasad równościowych w ramach Funduszy Unijnych na lata 2021-2027;
- W ramach szkoleń Wykonawca zapewni dokumentację wszystkich szkoleń:
  1) Listy obecności uczestników szkoleń;
  2) Listy odbioru certyfikatów o ukończonych szkoleniach;
  3) Dzienniki szkoleń zawierające informacje na temat przebiegu oraz o zakresie merytorycznym szkoleń, podpisane przez osobę prowadzącą szkolenia;
  4) Dokumentację fotograficzną z przeprowadzonych szkoleń (forma elektroniczna);
- Wykonawca zobowiązuje się w terminie 5 dni od dnia podpisania umowy dostarczyć Zamawiającemu:
  1) Proponowane terminy szkoleń;
  2) Szczegółowy zakres merytoryczny szkoleń;
  3) Harmonogram szkoleń;
- Wykonawca zobowiązany jest do współpracy i konsultacji z Zamawiającym oraz do wprowadzania poprawek do sporządzonej dokumentacji zgodnie z sugestiami Zamawiającego na każdym etapie realizacji zamówienia;
- Wykonawca przed przystąpieniem do realizacji zamówienia zobligowany jest do przeprowadzenia wśród uczestników szkoleń ankiety potrzeb w zakresie zapewnienia dostępności dla osób ze szczególnymi potrzebami;
- Wykonawca w trakcie realizacji zamówienia zobligowany jest do zapewnienia dostępności dla osób ze szczególnymi potrzebami.
- Wymagania dodatkowe:
- Wykonawca do realizacji zadania oddeleguje osobę, gdzie:
  1) prelegent posiada certyfikat Bezpieczeństwa Informacji zgodnie z normą PN-EN ISO 27001 – Zamawiający na etapie oceny ofert przyzna dodatkowe 10 pkt.

**Wymagane dokumenty:**

- Wykonawca składa poprawnie wypełniony formularz oferty;
- Wykonawca, jeżeli posiada, to wraz z ofertą przedłoży certyfikaty Bezpieczeństwa Informacji zgodnie z normą PN-EN ISO 27001;

**Informacje Zamawiającego:**

- Zamawiający informuje, że sala konferencyjna w której planowane są szkolenia stacjonarne wyposażona jest w ekran projekcyjny, projektor, monitor dotykowy o wielkości 75” oraz dostęp do Internetu bezprzewodowego;

- Zamawiający zastrzega sobie prawo do wzywania do wyjaśnień Wykonawców w celu potwierdzenia referencji osób oraz przedmiotu szkoleń bezpośrednio w podmiotach, na rzecz których Wykonawca szkolenia realizował,
- Zamawiający zastrzega sobie prawo do wzywania do wyjaśnień Wykonawców w celu potwierdzenia referencji osób oraz przedmiotu szkoleń bezpośrednio poprzez przedłożenie referencji imiennych dla osób, które zostaną wskazane do realizacji szkoleń, wystawionych przez podmioty, u których wskazana osoba realizowała szkolenia,

**MINIMALNY ZAKRES I TEMATYKA SZKOLEŃ:**

**OCHRONA DANYCH OSOBOWYCH A CYBERBEZPIECZEŃSTWO**

1. Przepisy / akty prawne:
   - podstawowe akty prawne (RODO, UODO, KRI, KSC, NIS2)
   - co to są dane osobowe, typy danych, kto musi dbać o dane;
   - czym jest przetwarzanie danych, zasady przetwarzania;
   - dane wrażliwe, bezpieczeństwo, dostęp z i spoza obszaru przetwarzania;
   - ochrona danych a dostęp do informacji publicznej;
   - zgodność z prawem, warunki wyrażenia zgody, zgoda wyrażona przez dzieci;
   - obowiązki informacyjne;
   - prawa osób;
   - incydenty i naruszenia;
2. Zachowania:
   - rozmowy;
   - przekazywanie informacji w rozmowie bezpośredniej i telefonicznej, poczta i emaile; wysyłka listów tradycyjnych, szyfrowanie załączników e-mail i przekazywanie haseł;
   - bezpieczeństwo dokumentów, zostawianie dokumentów bez opieki (w tym zasady postępowania w przypadku konieczności chwilowego opuszczenia pomieszczenia, gdy pracownik przebywa sam na sam z klientem);
   - polityka kluczy - dostępy do pomieszczeń;
   - ,,żądania" osób lub instytucji danych osobowych;
   - korzystanie z komputerów służbowych;
   - zapisywanie danych w folderach;
   - hasła do komputerów i do programów użytkowych - indywidualizacja i zakaz udostępniania;
   - archiwizacja dokumentów i czyszczenie dysków - kasowanie danych z poczty i dysku-kosz;
   - przechowywanie danych;
   - emaile z potwierdzonych źródeł;
   - UDW;
3. Odpowiedzialność za naruszenie przepisów RODO:
   - odpowiedzialność ADO - administracyjna, cywilna, karna;
   - górne granice kar administracyjnych;

- odpowiedzialność ADO z ustawy o finansach publicznych w przypadku nałożenia kary administracyjnej tj. z tytułu naruszenia dyscypliny finansów publicznych;
- odpowiedzialność pracowników, których działania doprowadziły do odpowiedzialności ADO tj. ciężkie naruszenie obowiązków pracowniczych i związana z tym odpowiedzialność dyscyplinarna (Kodeks pracy i inne ustawy regulujące kwestie pracownicze w jednostkach)

4. Wprowadzenie do SZBI
   - PBI a SZBI;
   - Przegląd Systemu Zarządzania Bezpieczeństwem Informacji
   - Znaczenie SZBI dla organizacji
5. Rozpoznawanie i Kwalifikacja Incydentów Cyberbezpieczeństwa
   - Definicja incydentu cyberbezpieczeństwa
   - Typy incydentów i ich charakterystyka
   - Przegląd narzędzi i technik identyfikacji incydentów
6. Protokoły Postępowania przy Incydentach
   - Przygotowanie planu reagowania na incydenty
   - Etapy postępowania: od identyfikacji po eliminację skutków
   - Przypadek praktyczny: symulacja reagowania na incydent
7. Komunikacja i Raportowanie w Kontekście Incydentów
   - Wymagania dotyczące raportowania incydentów
   - Efektywna komunikacja wewnętrzna i zewnętrzna podczas kryzysu
   - Przykłady dokumentacji i raportów incydentów
   - Wymiana doświadczeń i rozwiązań między uczestnikami
   - Dyskusja na temat najnowszych trendów w SZBI

**CYBERBEZPIECZEŃSTWO – PHISHING, RANSOMWARE, INNE ZAGROŻENIAW SIECI**

1. Wprowadzenie do Cyberbezpieczeństwa
   - Kluczowe pojęcia i zagrożenia w cyberprzestrzeni;
   - Przegląd dzisiejszej agendy i celów szkolenia;
2. Phishing: Rozpoznawanie i Reagowanie
   - Definicja i rodzaje phishingu (spear phishing, whaling, vishing, smishing pharming spoofing spim scam);
   - Analiza przypadków: Jak rozpoznać podejrzane e-maile, wiadomości, połączenia;
3. Warsztaty: Symulacja Ataków Phishingowych
   - Praktyczne ćwiczenia w grupach;
   - Analiza próbek phishingowych i próba identyfikacji zagrożeń;
   - Wykorzystanie narzędzi do symulacji i testowania reakcji;
4. Ransomware: Mechanizmy i Sposoby Obrony
   - Przegląd różnych typów ransomware;
   - Analiza przypadków: Jak ransomware infekuje systemy i jakie są jego skutki;
   - Sposoby zapobiegania atakom ransomware: kopie zapasowe, aktualizacje, sandboxing
5. Inne zagrożenia w sieci
   - Niebezpieczne linki / wiadomości SMS / e-mail

- Dostęp zdalny a bankowość elektroniczna
- Sztuczna inteligencja
- Deep Fake

6. Dyskusja - pytania i odpowiedzi
   - Odpowiedzi na pytania uczestników szkolenia
   - Dyskusja na temat najnowszych trendów i rozwiązań w cyberbezpieczeństwie

**CYBERBEZPIECZEŃSTWO - NARZĘDZIA CYBERBEZPIECZEŃSTWA – JAK BEZPIECZNIE PRACOWAĆ, TOŻSAMOŚĆ ELEKTRONICZNA**

1. Wprowadzenie do Narzędzi Cyberbezpieczeństwa
   - Przegląd kluczowych pojęć i znaczenie bezpieczeństwa cyfrowego;
   - Cel szkolenia i przegląd agendy;
2. Wykorzystanie danych
   - Wykorzystanie pozyskanych danych przez cyberprzestępców (szantaże, korzyści majątkowe);
3. Pomoc zdalna
   - Czym jest i jak działa
   - Pomoc zdalna a obowiązujące przepisy
   - Dobre praktyki
4. Szyfrowanie Danych i Bezpieczne Przechowywanie
   - Podstawy szyfrowania danych
   - Narzędzia do szyfrowania dysków, plików, załączników w poczcie elektronicznej
   - Praktyczne ćwiczenia: Szyfrowanie plików na różnych systemach operacyjnych
5. Bezpieczne Przeglądanie Internetu i VPN
6. Dyskusja - pytania i odpowiedzi
   - Odpowiedzi na pytania uczestników szkolenia

**SZKOLENIA SPECJALISTYCZNE DLA KADRY ZARZĄDZAJĄCEJ URZĘDU Z ZAKRESU CYBERBEZPIECZEŃSTWA**

1. Wstęp do bezpieczeństwa w cyberprzestrzenii;
   - Akty Prawne;
   - Krajowy System Cyberbezpieczeństwa;
   - Analiza ataków cybernetycznych;
   - Najpopularniejsze zagrożenia;
   - Przewodnik po metodach obrony instytucji;
   - Cyberbezpieczeństwo osobiste;
2. Postępowanie w pracy;
   - ABC higieny pracy w cyberprzestrzeni;
   - Bezpieczeństwo pracy zdalnej;
   - Ataki socjotechniczne - czyli niewinne „wyłudzanie” danych
   - Kampanie Phishingowe
   - Opłacalność ataków DoS/DDoS wymierzonych w konkretną instytucję

3. Aktualne zagrożenia wynikające z wojny w Ukrainie·
4. Dyskusja - pytania i odpowiedzi
   - Odpowiedzi na pytania uczestników szkolenia

**2. Część 2 – Usługa szkolenia e-lerningowego na dedykowanej platformie internetowej (szkoleniowej):**

**Charakterystyka ogólna:** Platforma szkoleniowa zawierająca minimum 4 szkolenia, dostępne w języku polskim w postaci prezentacji, zakończonych testami lub quizami sprawdzającymi przyswojenie przedstawianego materiału merytorycznego. Na platformie przez 12 miesięcy od kwietnia 2025 do marca 2026. Wykonawca udostępni szkolenia e-learningowe: ochrona danych osobowych, cyberbezpieczeństwo, sygnaliści, skrócony kurs ochrony danych osobowych. Wykonawca założy konta uczestnikom szkolenia.

**Liczba uczestników:** Zamawiający przewiduje łączną liczbę uczestników szkoleń w ilości ok. 30 osób**.**

**Dostępność platformy:** Platforma elearningowa musi być dostępna dla wszystkich uczestników przez 24h na dobę, przez okres 12 m-cy od daty podpisania umowy.

**Planowane terminy szkoleń:** Termin świadczenie szkoleń elearningowych: dostęp do platformy e-learningowej wraz ze szkoleniami ważny przez 12 miesięcy od kwietnia 2025 do marca 2026.

**Minimalna dostępność szkoleń:** Na platformie elearningowej Wykonawca ustawi dostępność szkolenia ochrona danych osobowych w lipcu 2025, cyberbezpieczeństwo we wrześniu 2025, sygnaliści w listopadzie 2025, skrócony kurs ochrony danych osobowych utrwalający wiedzę w lutym 2026.

**Szkolenie dostępne na platformie musi spełniać następujące wymogi:**

1) Być responsywne tzn. dostosować wyświetlanie do komputera oraz tabletu – w pionie i poziomie, i telefonu - w pionie i poziomie. Nie dopuszczane są kursu przeskalowane, które otwierają się na urządzeniach bez dostawania treści szkolenia do wysokości wyświetlacza komputera, tabletu i telefonu.
2) Zablokowany test tzn. uczestnik nie może przejść do części kursu zawierającej test sprawdzający wiedzę, bez zapoznania się z informacjami przedstawionymi na ekranach poprzedzających test np.: w postaci rozwijanych kart, okien pop-up, markerów, wyświetlonych pytań i odpowiedzi.
3) Być interaktywne tzn. muszą angażować uczestnika poprzez zapewnienie możliwości klikania, zapoznawania się z materiałami dodatkowymi, rozwijania i otwierania okien z informacjami oraz udzielania odpowiedzi na zadawane pytania.
4) Szkolenie musi się kończyć testem, w którym zostaną użyte pytania jednokrotnego wyboru, wielokrotnego wyboru, prawda/fałsz.
5) Test musi zakończyć się podsumowaniem wyniku uzyskanego przez uczestnika szkolenia w postaci wyniku procentowego oraz informacji o uzyskaniu pozytywnej lub negatywnej oceny końcowej.
6) Uczestnik musi otrzymać informację zwrotną w postaci określenia, na które pytania odpowiedział poprawnie, a na które błędnie.
7) Szkolenia muszą zapewniać zakres tematyczny co najmniej w ujęciu:

- Podstawy bezpiecznego internetu;
- Bezpieczeństwo poczty;
- Załączniki w poczcie elektronicznej;
- Ochrona przed złośliwym oprogramowaniem;
- Bezpieczeństwo danych osobowych RODO/GDRP;
- Bezpieczne hasła i menedżery haseł;
- Bezpieczeństwo urządzeń mobilnych;
- Uwierzytelnianie wieloskładnikowe (MFA);
- Bezpieczna praca zdalna;
- Bezpieczna praca w biurze;
- Zagrożenia w mediach społecznościowych;
- Ochrona przed phishingiem;
- Socjotechnika – metody i techniki manipulacji człowiekiem;
- Zakupy w internecie;

8) Dedykowana platforma dostarczająca raporty obejmujące minimum:
   - liczbę wizyt na platformie w podziale na użytkownika i wszystkich użytkowników;
   - czas spędzony platformie w podziale na użytkownika i wszystkich użytkowników;
   - czas spędzony w kursie z opcją filtrowania po kursie, kohorcie, użytkowniku;
   - lista nieaktywnych użytkowników;
   - rozkład czasowy korzystania użytkowników z platformy w ujęciu tygodniowym i 24 godzinnym;
   - przegląd ocen w kursie z opcją filtrowania po kohortach, kursie, użytkowniku;
   - popularność kursów na platformie w ujęciu zapisów, odwiedzin kursantów;
   - wszystkie powyższe raporty muszą być prezentowane graficznie np.: tabela, lista, wykres oraz umożliwiać pobranie danych w formie pliku, np.: PDF lub JPG lub SVG.
9) Udostępniona platforma musi zostać dostosowana graficznie do layoutu Zamawiającego w zakresie minimalnym tj.:
   - logo i favicon,
   - wpisy w menu głównym,
   - zmiany treści stopki,
   - czcionki nagłówków i tekstów,
   - kolorystyka przycisków,
   - strony z treściami zgód (RODO, marketing) wymaganymi przy pierwszym logowaniu
   - stronę logowania do platformy (tło, logo).
   - jeśli zajdzie potrzeba stworzymy stronę główną platformy widoczną dla kursanta
   - przed zalogowaniem się do platformy.
   - Zmiany wyglądu i treści wiadomości powitalnych wychodzących z platformy (logo, kolor tła, opis, czcionka, stroka emaila),

**Wymagania:**

- Środowisko pracy: Platforma e-learningowa musi być dostępna z poziomu przeglądarek internetowych Firefox, Chrome, Edge dla systemów Windows 10/11 w aktualnych wersjach;
- Zasady działania pomocy technicznej: Zgłoszenia pomocy technicznej i komunikacja z Wykonawcą będą przyjmowane w języku polskim w trybie 24x7 przez funkcję chat

dostępną na platformie oraz infolinię w języku polskim 8x5. Czas reakcji Wykonawcy nie może być dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w polu chat.

**SLA – gwarantowany poziom świadczenia usług:**

- Dostępność platformy – na poziomie minimum 99,8% przez cały okres realizacji zamówienia;
- Nielimitowany transfer danych;
- Codzienna kopia zapasowa danych – przetrzymywana 28 dni
- Platforma zabezpieczona certyfikatem SSL;
- Minimalna ilość łącznych dostępów uczestników do platformy w tym samym czasie na poziomie 100%;
- Zobowiązania Wykonawcy:
- Wykonawca wyda każdemu uczestnikowi szkolenia certyfikat o ukończeniu szkolenia;

**Dostępność platformy:**

Platforma elearningowa musi być dostępna dla wszystkich uczestników przez 24h na dobę.