

ZP.271.2.16.2024

**Opis przedmiotu zamówienia (OPZ)
dla części 1 – Cyberbezpieczeństwo**

1. Szkolenia z zakresu cyberbezpieczeństwa wszystkich pracowników Urzędu Gminy Radymno celem podniesienia poziomu wiedzy oraz kompetencji w wyżej wymienionym zakresie.

Przedmiotem zamówienia jest usługa szkoleniowa e-learningowa na platformie szkoleniowej wykonawcy dla 60 pracowników Urzędu Gminy Radymno z 12 miesięcznym dostępem do modułów szkoleniowych w zakresie cyberbezpieczeństwa.

Kod i nazwa zamówienia według Wspólnego Słownika Zamówień (CPV):

80500000-9 – usługi szkoleniowe

80420000-4 – usługi e-learning

1. Minimalny zakres tematyczny:

- ataki socjotechniczne;
- polityka haseł;
- złośliwe oprogramowanie;
- phishing;
- cyberhigiena;
- wycieki informacji;
- poczta i załączniki;
- elementy ochrony danych osobowych.

2. Specyfikacja dostępu do platformy:

- Dostęp do platformy bez konieczności instalacji dedykowanego komponentu oprogramowania typu desktop, w systemach operacyjnych Windows i Linux, w przeglądarkach internetowych - bez konieczności instalacji dodatkowych komponentów – Microsoft Edge, Mozilla Firefox, Google Chrome;
- Szyfrowanie SSL we wszystkich przypadkach, gdy wysyłane są dane osobowe. Szyfrowanie SSL musi być widoczne w pasku adresu przeglądarki za pomocą przedrostka „https://”. Certyfikat wykorzystany do szyfrowania SSL musi być rozpoznawany jako zaufany w najnowszych wersjach przeglądarek zdefiniowanych do obsługi platformy szkoleniowej;
- Polskojęzyczny interfejs użytkownika o intuicyjnej obsłudze;
- Możliwość odbycia szkolenia w formie e-learningowej w ciągu co najmniej 12 miesięcy od daty zakupu usługi;
- Możliwość utworzenia danych dostępowych dla poszczególnych uczestników;
- Możliwość wygenerowania imiennych zaświadczeń (certyfikatów) o ukończeniu szkolenia dla każdego z uczestników;
- Platforma powinna posiadać ćwiczenia praktyczne oraz materiały wideo. Nie może to być wyłącznie pokaz slajdów w formie prezentacji;

3. Termin realizacji zamówienia:

Wykonawca jest zobowiązany udostępnić szkolenie on-line na platformie w terminie 7 dni od podpisania umowy.

4. Cena ofertowa powinna zawierać w sobie wszelkie koszty niezbędne do zrealizowania zamówienia. Wykonawca sporządzając ofertę powinien przewidzieć wszelkie okoliczności mogące mieć wpływ na cenę.

5. Szkolenia zrealizowane miałyby być w formie usługi szkoleniowej e-learningowej na platformie szkoleniowej wykonawcy dla 60 pracowników Urzędu Gminy z 12 miesięcznym dostępem do modułów szkoleniowych

6. Szkolenie zakończone egzaminem kontrolnym wraz z wydaniem certyfikatu imiennego z jego przeprowadzenia

7. Platforma zapewnia użytkownikowi:

- a) aktualne materiały z zakresu cyberbezpieczeństwa z nielimitowanym dostępem,
- b) testy online,
- c) moduły szkoleniowe z nielimitowanym dostępem
- d) imienny certyfikat,
- e) dostęp do logowania oraz bazy wiedzy przez całą dobę
- f) pomoc techniczną

2. Opracowanie/ aktualizacja dokumentacji systemu zarządzania bezpieczeństwem informacji (SZBI)

Kompleksowe wykonaniu zamówienia dotyczącego opracowania/aktualizacji dokumentacji SZBI, przeglądu SZBI, przeprowadzenie audytu KRI, ksc i testów podatności, przeprowadzenie końcowego audytu wdrożonego systemu zarządzania bezpieczeństwem informacji, szkolenia dla pracowników i kierownictwa z SZBI oraz podstaw ISO 27001 w Urzędzie Gminy Radymno.

Opis poszczególnych zadań realizowanych w ramach zamówienia:

Lp.	Zakres	szt./kpl/os.
1	SZBI: Uaktualnienie dokumentacji, w tym opracowanie niezbędnych procedur do wymagań KRI/KSC, wdrożenie SZBI	1
2	Szkolenie dla pracowników i kierownictwa z SZBI oraz podstaw ISO 27001	60
3	Audyt KRI, ksc i testy podatności w 2024 r. w UG Radymno	1
4	Przegląd SZBI w 2025 r. dla UG Radymno	1
5	Końcowy audyt zgodności przeprowadzany przez uprawnionego audytora wiodącego w UG Radymno	1

Ad.1

SZBI: Uaktualnienie dokumentacji, w tym opracowanie niezbędnych procedur do wymagań KRI/KSC, wdrożenie SZBI

1. Uaktualnienie posiadanej dokumentacji i procedur Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) - zgodnie z przepisami prawa unijnego, krajowego oraz normami odnoszącymi się do bezpieczeństwa informacji (np. ISO 27001, ISO 27002 dla systemów informatycznych, **ISO 22301**).
2. Dokumentacja SZBI musi być opracowana na podstawie Polskiej Normy PN-ISO/IEC 27001, na podstawie Polskich Norm związanych z tą normą, w tym: PN-ISO/IEC 27002 – w odniesieniu do ustanawiania zabezpieczeń, PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem; PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.
3. Opracowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (w skład czego mogą wchodzić różne polityki i procedury)
4. Opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (dalej zwanej „SZBI”), w skład której wchodzi następujące dokumenty:
 - a. Polityka Bezpieczeństwa Informacji;
 - b. Polityka zarządzania ciągłością działania;
 - c. Procedura zarządzania incydentami cyberbezpieczeństwa
 - d. Procedura zarządzania ryzykiem;
 - e. Procedura kontroli dostępu do informacji i polityka haseł
 - f. Procedura zasobów ludzkich

- g. Procedura bezpieczeństwa fizycznego, organizacyjnego i technicznego
 - h. Procedura pracy zdalnej
 - i. Procedura profilaktyki antywirusowej
 - j. Procedura kopii zapasowej
 - k. Procedura współpracy z dostawcami
 - l. Procedura zarządzania podatnościami
 - m. Procedura zarządzania incydentami
 - n. Procedura audytu bezpieczeństwa informacji
5. Wdrożenie opracowanej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)
 6. Wykonawca zobowiązany jest do udziału w końcowym audycie zgodności przeprowadzonym przez uprawnionego audytora wiodącego w Urzędzie Gminy Radymno, który zostanie zlecony przez Zamawiającego w 2025 r.
 7. W sytuacji, gdy końcowy audyt zgodności w 2025 r. przeprowadzany przez audytora wiodącego stwierdzi nieprawidłowości lub braki wynikające z winy Wykonawcy, wykonawca uaktualnienia SZBI zobowiązany będzie dostosować dokumentację do zaleceń po audytowych.

Ad.2

Szkolenie dla pracowników i kierownictwa z SZBI oraz podstaw ISO 27001

Przeprowadzenie szkoleń dla pracowników i kierownictwa z SZBI oraz podstaw ISO 27001 – szkolenie w formie zdalnej lub stacjonarnej dla 60 osób, w podziałach na min. 2 grupy, rozłożone na 2 dni robocze (jedna grupa = jeden dzień szkolenia), czas trwania co najmniej 5 godzin/każda grupa.

Miejsce szkolenia Sala Narad Urzędu Gminy Radymno (Radymno, ul. Lwowska 38) lub forma zdalna. Szkolenie zorganizowane w godz. 8.00 – 15.00, od poniedziałku do piątku.

Program szkolenia przygotowuje Wykonawca, program ma być dostosowany do tematyki szkolenia oraz przygotowany pod kątem uczestników szkolenia tj. pracownicy Urzędu Gminy Radymno. Program szkolenia musi uzyskać akceptację Zamawiającego.

Szkolenie zakończone uzyskaniem zaświadczenia o udziale w szkoleniu dla każdego pracownika/kierownika uczestniczącego w szkoleniu.

Ad.3

Audyt KRI, ksc i testy podatności w 2024 r. w UG Radymno

Audyt musi być dostosowany do wymagań rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, zgodny z wymogami ustawy KSC.

Audyt musi być przeprowadzony przez osobę posiadającą certyfikat uprawniający do przeprowadzenia audytu, o którym mowa w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.

Minimalny zakres zadania:

- Analiza wstępna stanu bezpieczeństwa informacji w UG Radymno w zakresie objętym audytem
- Identyfikacja obowiązujących wymagań, ocena istniejących systemów i procedur
- Zebranie wstępnych odpowiedzi i dowodów audytowych rekomendacje dotyczące działań naprawczych i usprawnień
- raport z audytu
- wsparcie w dostosowaniu dokumentacji i procedur obowiązujących w UG Radymno
- Przeprowadzenie testów podatności w UG Radymno

- Wykonanie audytu zgodnie z wymaganiami art. 21 - 23 ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC) i § 19 rozporządzenia w sprawie Krajowych Ram Interoperacyjności (KRI)
- Ocena zgodności z Krajowymi Ramami Interoperacyjności (KRI) / Krajowym Systemie Cyberbezpieczeństwa (KSC)
- Opracowanie raportu z audytu wskazującego wykryte podatności oraz błędy wraz rekomendacjami działań naprawczych i korygujących umożliwiających minimalizację zidentyfikowanych ryzyk
- Wsparcie po audytowe, które polegać ma m.in. na udzielaniu informacji na temat audytowanych elementów wynikających z raportu, wsparcie w dostosowaniu dokumentacji i procedur obowiązujących w UG Radymno .
- Audyt musi być wykonany przez osoby uprawnione przepisami prawa.

Ad.4

Przegląd SZBI w 2025 r. dla UG Radymno

Aktualizacja przygotowanej w 2024 r. dokumentacji SZBI, dostosowanie dokumentów do aktualnych wymagań.

Przegląd SZBI musi obejmować co najmniej:

- Sprawdzenie aktualności SZBI pod względem prawnym
- Sprawdzenie funkcjonalności SZBI - dostosowania do UG Radymno
- Ocena obecnego stanu Systemu Zarządzania Bezpieczeństwem Informacji w UG Radymno
- Analiza zgodności z wymaganiami ISO 27001 i ISO 27002.
- Identyfikacja luk i potencjalnych zagrożeń
- Raport z wykonanych prac zawierający niezgodności oraz rekomendacje.

Ad.5

Końcowy audyt zgodności przeprowadzany przez uprawnionego audytora wiodącego w UG Radymno

Wykonawca zobowiązany jest do opracowania audytu końcowego, który jest warunkiem prawidłowego rozliczenia projektu pn. „Cyberbezpieczna Gmina Radymno”.

Wykonawca jest zobowiązany do przeprowadzenia audytu wdrożonego systemu zarządzania bezpieczeństwem informacji w związku z obowiązkiem ciążącym na kierownictwie podmiotu publicznego zgodnie z zapisami w § 20 ust. 2 pkt 14 rozporządzenia w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2017 poz. 2247 z późn.zm.), zwanego dalej „rozporządzeniem KRI”, zgodnie z poniższymi warunkami:

- 1) zakres audytu systemu bezpieczeństwa informacji wdrożonego w urzędzie JST obejmuje zgodność z kryteriami zawartymi w § 20 ust. 2 ww. rozporządzenia KRI lub zgodność z wymaganiami normy PN-ISO/IEC 27001
- 2) raport z audytu zostanie podpisany przez audytora dokonującego audyt systemu bezpieczeństwa informacji wdrożonego w urzędzie JST i dostarczony do Zamawiającego
- 3) audyt systemu bezpieczeństwa informacji wdrożonego w Urzędzie Gminy Radymno zostanie przeprowadzony przez:
 - a) audytora zewnętrznego posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz. 1999 z późn. zm.)
 - lub
 - b) audytora wewnętrznego posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do

przeprowadzenia audytu (Dz.U.2018 poz. 1999 z późn. zm.) lub będącego audytorem zewnętrznym systemu zarządzania bezpieczeństwem informacji według normy PN-ISO/IEC 27001;

Przeprowadzenie audytu zgodności musi obejmować co najmniej:

- Analiza końcowa stanu bezpieczeństwa informacji w urzędzie w zakresie objętym audytem
- Identyfikacja obowiązujących wymagań, ocena istniejących systemów i procedur
- Zebranie końcowych odpowiedzi i dowodów audytowych
- Wspólne zdefiniowanie rekomendowanych działań korygujących w zakresie objętym audytem, rekomendacje dotyczące działań naprawczych i usprawnień
- Raport z audytu
- Wsparcie w dostosowaniu dokumentacji i procedur obowiązujących w UG Radymno

Wykonanie audytu zgodnie z wymaganiami art. 21 - 23 ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC) i § 19 rozporządzenia w sprawie Krajowych Ram Interoperacyjności (KRI)

Ocena zgodności z Krajowymi Ramami Interoperacyjności (KRI) / Krajowym Systemie Cyberbezpieczeństwa (KSC)

Opracowanie raportu z audytu wskazującego wykryte podatności oraz błędy wraz rekomendacjami działań naprawczych i korygujących

Wsparcie poaudytowe, które polegać ma m.in. na: udzielanie informacji na temat audytowanych elementów wynikających z raportu.

Audyt musi być wykonany przez osoby uprawnione przepisami prawa.

W ramach zamówienia Wykonawca zobowiązany jest do opracowania „Ankiety dojrzałości Cyberbezpieczeństwa” na podstawie opracowanej ankiety przed realizacją projektu.

Ankieta jest załącznikiem nr 6 Ankieta Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego (i Jednostkach Podległych) do regulaminu konkursu grantowego pn. „Cyberbezpieczny Samorząd”, Priorytet II: Zaawansowane usługi cyfrowe, działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa, Fundusze Europejskie na Rozwój Cyfrowy 2021 – 2027 (FERC).