Załącznik nr 1

Szczegółowy opis przedmiotu zamówienia (SOPZ)

1. Przedmiotem zamówienia są szkolenia dla kadry zarządzającej i informatyków Starostwa Powiatowego w Tomaszowie Mazowieckim w ramach projektu dofinansowanego w konkursie grantowym „Cyberbezpieczny Samorząd" w ramach programu Fundusze Europejskie na Rozwój Cyfrowy (FERC).
2. W zakres zadania nr 1 wchodzą **„Szkolenia specjalistyczne dla kadry zarządzającej w zakresie zastosowanych środków bezpieczeństwa i skali zagrożeń systemów IT"** (3 szkolenia). Do przedmiotowych szkoleń należą:
   2.1. Szkolenie „Bezpieczny Samorząd – Cyberbezpieczeństwo dla kadry zarządzającej" (przeznaczone dla maksymalnie 30 uczestników).
   2.2. Szkolenie „Dyrektywa NIS2 i strategie Analizy Ryzyka" (przeznaczone dla maksymalnie 30 uczestników).
   2.3. Szkolenie „System Zarządzania Bezpieczeństwem Informacji" (przeznaczone dla maksymalnie 30 uczestników).
3. Wykonawca zobowiązany będzie do przeprowadzenia szkoleń w terminie do 10.04.2026r.
4. Szkolenia prowadzone będą w trybie stacjonarnym, podczas których prowadzący instruktor będzie do dyspozycji uczestników przez cały czas trwania szkolenia.
5. Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego dziennego harmonogramu prac oraz zakresu merytorycznego szkolenia, dostarczonego przez Wykonawcę Zamawiającemu nie później niż 3 dni przed rozpoczęciem szkolenia.
6. Szkolenia odbędą się w sali konferencyjnej Starostwa Powiatowego w Tomaszowie Maz. w grupie maks. 30 osobowej. Minimalny czas trwania szkolenia to 7 godzin zegarowych w zakresie godzinowym 8:00 - 15:30 w dni robocze (tj. poniedziałek-piątek).
7. W ramach organizacji szkoleń Wykonawca zapewni:
   7.1. Materiały szkoleniowe, obejmujące szczegółowy zakres szkolenia oraz materiały merytoryczne (np. skrypty, podręczniki, zeszyty informacyjne, broszury) w formie papierowej/elektronicznej, zawierające szczegółowe informacje, które będą omawiane podczas szkolenia. Ponadto, uczestnicy otrzymają materiały pisarskie (jeżeli istnieje taka konieczność), w tym zeszyty, długopisy, ołówki itp. Materiały szkoleniowe przekazywane są nieodpłatnie Uczestnikom na własność. 2 egzemplarze materiałów szkoleniowych zostaną przekazane Zamawiającemu w celach archiwalnych.
   7.2. Warunki pracy uczestników i Wykonawcy w trakcie trwania szkolenia zgodne z przepisami bezpieczeństwa i higieny pracy.
   7.3. Prezentacje multimedialne, tablice i inne artykuły niezbędne do prowadzenia szkolenia.
   7.4. Kadrę trenerską posiadającą wiedzę i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkoleń.
   7.5. Prowadzenie dokumentacji wszystkich szkoleń w jednakowy sposób. Na dokumentację szkolenia składają się:

7.5.1. Lista obecności Uczestników szkolenia (dzienna, wypełniana oddzielnie każdego dnia szkolenia).

7.5.2. Lista odbioru potwierdzona przez Uczestników szkolenia, imiennych certyfikatów potwierdzających uczestnictwo w szkoleniu.

7.5.3. Sporządzony przez kadrę trenerską dziennik zajęć, zawierający szczegółowe informacje na temat przebiegu oraz zakresu merytorycznego szkolenia, podpisany po zakończeniu szkolenia przez prowadzącego szkolenie.

7.6. Dla każdego uczestnika szkolenia, wydrukowany imienny certyfikat potwierdzający uczestnictwo w szkoleniu.

7.7. **Programy szkoleń.**

7.7.1. Program szkolenia „Bezpieczny Samorząd – Cyberbezpieczeństwo dla kadry zarządzającej".

7.7.1.1. Podstawy cyberbezpieczeństwa (podstawowe pojęcia i zasady działania).

7.7.1.2. Ocena ryzyka, w tym metody identyfikacji i analizy ryzyka związanego z IT, środki zaradcze w celu minimalizacji ryzyka.

7.7.1.3. Audyt wewnętrzny (cyberbezpieczeństwa) i raportowanie zgodności z przepisami.

7.7.1.4. Przegląd najpopularniejszych zagrożeń (w tym rodzaje ataków, ransomware i malware, phishing, oszustwa i wyłudzenia z uwzględnieniem oszustwa typu Business E-mail Compromise, atak telefoniczny, spoofing, atak odwrócony – zmuszenie ofiary do szukania pomocy u atakującego, przekręt nigeryjski, wyłudzenia BLIK, oszustwo na dyrektora/prezesa).

7.7.1.5. Znaczenie cyberbezpieczeństwa dla jednostki samorządu terytorialnego.

7.7.1.6. Przegląd aktualnych zagrożeń i trendów w cyberprzestrzeni.

7.7.1.7. Analiza przepisów rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2024 poz. 773) i ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2024 poz. 1077 z późn. zm.).

7.7.1.8. Zasady postępowania w razie wprowadzenia stopni alarmowych CRP dotyczących zagrożeń w cyberprzestrzeni.

7.7.1.9. Obowiązki jednostek samorządu terytorialnego wynikające z przepisów.

7.7.1.10. Metody identyfikacji i oceny ryzyka.

7.7.1.11. Tworzenie i implementacja polityk ochrony danych.

7.7.1.12. Standardy i najlepsze praktyki postępowania w celu zapewnienia cyberbezpieczeństwa w urzędzie, cyberhigiena.

7.7.1.13. Profilaktyka cyberbezpieczeństwa w urzędzie, standardy i najlepsze praktyki w tym w zakresie bezpieczeństwa urządzeń i bezpieczeństwa fizycznego.

7.7.1.14. Sposoby podnoszenia świadomości pracowników Urzędu w zakresie cyberbezpieczeństwa i testowania odporności Urzędu na różnego rodzaju ataki.

7.7.1.15. Umiejętność skutecznej komunikacji z zespołem, z innymi komórkami urzędu i jednostek podległych oraz z interesariuszami zewnętrznymi w sprawach cyberbezpieczeństwa.

7.7.1.16. Procesy i procedury zarządzania incydentami oraz role poszczególnych pracowników.

7.7.1.17. Rola kadry kierowniczej w zakresie cyberbezpieczeństwa (w tym w sytuacjach kryzysowych).
7.7.1.18. Incydenty w kontekście zachowania ciągłości działania urzędu.
7.7.1.19. Przywództwo, motywowanie zespołu i promocja kultury bezpieczeństwa w urzędzie.
7.7.1.20. Ćwiczenia praktyczne:
- Rozpoznawaniem zagrożeń i reagowaniem na nie.
- Analizą rzeczywistych incydentów (studia przypadków).
- Zarządzaniem w sytuacjach kryzysowych (scenariusze codziennych zagrożeń).

7.7.2. Program szkolenia „Dyrektywa NIS2 i strategie Analizy Ryzyka":
7.7.2.1. Dokumentacja SZBI zgodna z normą ISO 27001:
- Omówienie kluczowych dokumentów wymaganych przez normę ISO 27001.
- Polityka bezpieczeństwa informacji i jej znaczenie w kontekście SZBI.
- Procedury i instrukcje operacyjne związane z bezpieczeństwem informacji.
- Rejestry i zapisy wymagane do utrzymania SZBI.
- Praktyczne wskazówki dotyczące tworzenia i zarządzania dokumentacją SZBI.
- Rola dokumentacji w procesie ciągłego doskonalenia SZBI.

7.7.2.2. Wprowadzenie do Dyrektywy NIS2:
- Kluczowe zmiany w porównaniu do poprzedniej dyrektywy NIS.
- Nowe wymagania i obowiązki dla operatorów usług kluczowych oraz dostawców usług cyfrowych.
- UKSC – obowiązujące przepisy prawne na terenie Polski.

7.7.2.3. Wymagania techniczne:
- Standardy i normy techniczne wymagane przez Dyrektywę NIS2
- Norma ISO 27001 a wymagania dyrektywy NIS2.
- Praktyczne aspekty implementacji zabezpieczeń technicznych w systemach informatycznych.

7.7.2.4. Wyzwania przed pracownikami:
- Identyfikacja i analiza głównych wyzwań związanych z cyberbezpieczeństwem w sektorze.
- Przykłady najlepszych praktyk i studia przypadków z innych organizacji z branży.

7.7.2.5. Praktyczne ćwiczenia i symulacje:
- Scenariusze incydentów cybernetycznych i reakcje na nie.
- Ćwiczenia z zakresu oceny ryzyka i zarządzania kryzysowego.

7.7.3. Program szkolenia „System Zarządzania Bezpieczeństwem Informacji":
7.7.3.1. Wprowadzenie:
- Pojęcie aktywów głównych i wspierających, bezpieczeństwa informacji.
- Systemowe podejście do zapewnienia bezpieczeństwa informacji – model PDCA.
- Normy rodziny ISO 27000 jako model Systemu Zarządzania Bezpieczeństwem Informacji.

7.7.3.2. Planowanie i wdrożenie systemu zarządzania
- Źródła wymagań i zaleceń – norma ISO 27001 oraz ISO 27002.

- Kontekst organizacji
- Przywództwo i polityka bezpieczeństwa.
- Role i odpowiedzialności.
- Cele bezpieczeństwa informacji.
- Planowane w oparciu o ryzyka i szanse.
- Niezbędne zasoby, świadomość i szkolenia.

7.7.3.3. Utrzymanie systemu zarządzania

- Pomiary i ocena systemu zarządzania bezpieczeństwem informacji.
- Audyt wewnętrzny.
- Przegląd systemu zarządzania.
- Doskonalenie systemu zarządzania.

7.7.3.4. Przegląd zabezpieczeń

- Omówienie zabezpieczeń z załącznika A normy ISO/IEC 27001:2022
- Przykładowe mierniki skuteczności zabezpieczeń

7.8. Wynagrodzenie za realizację zakończonej usługi, przekazane będzie po prawidłowym wykonaniu usługi i przekazaniu Zamawiającemu dokumentacji określonej w punkcie 7.5.

7.9. Uwagi dotyczące przetwarzania danych.

Wykonawca realizując przedmiot zamówienia jest zobligowany do zachowania w tajemnicy wszelkich informacji pozyskanych w sposób bezpośredni lub pośredni, dotyczących Powiatu Tomaszowskiego i pracowników Starostwa Powiatowego w Tomaszowie Maz., a w szczególności danych osobowych, informacji technicznych, ekonomicznych lub organizacyjnych. Zobowiązanie do zachowania poufności dotyczy wszelkich informacji udzielonych ustnie, pisemnie drogą elektroniczną lub w inny sposób w odpowiedzi na zapytania Wykonawcy w trakcie realizacji zadań szkoleniowych i jest bezterminowe.

Warunkiem podpisania umowy na realizację przedmiotu zamówienia będzie podpisanie z Zamawiającym oddzielnej umowy dotyczącej powierzenia przetwarzania danych osobowych.