

Załącznik nr 1.2 do SWZ**Opis przedmiotu zamówienia****Znak Sprawy: IP.271.1.2026****CZĘŚĆ I ZAMÓWIENIA – Wzmocnienie potencjału organizacyjnego – SZBI i szkolenia pracowników**

Przedmiotem zamówienia jest usługa kompleksowego opracowania, wdrożenia i przygotowania do certyfikacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnego z normą ISO/IEC 27001:2022, Krajowe Ramy Interoperacyjności - KRI, ustawą o Krajowym Systemie Cyberbezpieczeństwa - KSC, RODO i NIS2, a także przeprowadzenie szkoleń dla pracowników, audytów zgodności oraz testów penetracyjnych infrastruktury IT i OT (Operational Technology), w Urzędzie Gminy Urszulin w ramach programu Cyberbezpieczny Samorząd Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa Fundusze Europejskie Na Rozwój Cyfrowy 2021-2027 (Ferc).

W ramach zadania Wykonawca:

- 1) przygotowuje pełną dokumentację SZBI - polityki, procedury, rejestry aktywów, analizy ryzyka i plany ciągłości działania,
- 2) wdroży wymagania w organizacji i wesprze w przygotowaniu do audytu certyfikacyjnego,
- 1) przeszkoli kadrę kierowniczą i pracowników w zakresie bezpieczeństwa informacji i stosowania SZBI,
- 2) przeprowadzi audyty wstępne i powdrożeniowe zgodnie z ISO 27001, KRI i KSC,
- 3) zrealizuje testy penetracyjne infrastruktury sieciowej, aplikacyjnej, chmurowej i bezprzewodowej według standardów NIST, MITRE ATT&CK, CIS i OWASP dostarczając raport z wynikami i rekomendacjami naprawczymi.

Rezultatem będzie spójny i certyfikowalny SZBI, przeszkolony personel, raporty z audytów i testów penetracyjnych oraz podniesienie poziomu cyberbezpieczeństwa organizacji.

I. Opracowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji.

1. Poprzez opracowanie dokumentacji systemu należy rozumieć: przygotowanie przez Wykonawcę dokumentów od strony merytorycznej i formalnej do stanu, który pozwala przekazać dokumenty do jednostki certyfikującej przez Zamawiającego, bez podejmowania działań redakcyjnych lub innych ingerencji w treść dokumentu ze strony Zamawiającego.
2. Wykonawca na etapie prac wdrożeniowych, uzgadnia treść dokumentów z Zamawiającym.
3. Wykonawca gwarantuje, że dokumentacja systemu zarządzania bezpieczeństwem informacji jest zgodna z wymaganiami normy ISO/IEC 27001.
4. Zamawiający oczekuje od Wykonawcy przed przystąpieniem do prac opracowania dokumentacji przeprowadzenie audytu pozwalającego na zapoznanie się z dokumentacją obowiązującą u Zamawiającego i specyfiką pracy Gminy.
5. Zamawiający udostępni Wykonawcy wszystkie niezbędne materiały i udzieli odpowiedzi na pytania podczas realizacji przedmiotu zamówienia.
6. Wykonawca zobowiązany jest do zachowania w poufności informacji uzyskanych na etapie opracowania i wdrożenia SZBI u Zamawiającego na podstawie odrębnej umowy o Powierzenie danych osobowych.
7. W ramach zadania Wykonawca zobowiązuje się, do opracowania w szczególności :
 - a) Polityki bezpieczeństwa informacji - główny dokument określający cele i zasady ochrony informacji.
 - b) Ról i odpowiedzialności SZBI - przypisanie obowiązków administratorów, właścicieli procesów i danych.
 - c) Rejestru i klasyfikacji aktywów informacyjnych - wykaz systemów, danych, aplikacji i zasobów z przypisanymi właścicielami i poziomami ochrony.
 - d) Procedury zarządzania ryzykiem zgodnie z ISO 27005 i ISO 31000 - identyfikacja zagrożeń, ocena ryzyka, plan postępowania z ryzykiem.
 - e) Procedury bezpieczeństwa operacyjnego z uwzględnieniem:
 - polityki haseł i kontroli dostępu,
 - bezpiecznego korzystania z usług chmurowych,
 - procedury dla pracy zdalnej i BYOD,
 - zarządzanie incydentami i plan reagowania,
 - procedury ciągłości działania i plany awaryjne (BCP/DRP).

- f) Procedur i wzorów dokumentów audytu wewnętrznego, protokołów z przeglądu zarządzania.
 - g) Wytycznych do oceny i nadzoru dostawców oraz procedury transferu danych między organizacjami.
 - h) Instrukcji i formularzy operacyjnych dla codziennych działań związanych z bezpieczeństwem (np. przyjmowanie gości, dostęp do stref chronionych, przydzielanie uprawnień).
8. Wykonawca zobowiązuje się do udzielania wyjaśnień i konsultacji dotyczących wdrożonego SZBI oraz wprowadzenie ewentualnych zmian lub poprawek w dokumentacji SZBI w przypadku wykazania takiej konieczności.

II. Szkolenie dla pracowników i kierownictwa z SZBI oraz podstaw ISO 27001.

1. Cel szkolenia: Celem szkolenia jest podniesienie świadomości i wiedzy pracowników w zakresie obejmującym podstawy ISO 27001 oraz zasady działania Systemu Zarządzania Bezpieczeństwem Informacji.
2. Program szkolenia przygotowuje Wykonawca uwzględniając tematykę szkolenia oraz dokumentację wdrożeniową SZBI i przedstawia do akceptacji Zamawiającemu w terminie 2 dni przed terminem przeprowadzenia szkolenia.
3. Szkolenia stacjonarne lub online, w 3 grupach szkoleniowych, w tym jedna dla kadry kierowniczej
4. Warsztaty interaktywne, studia przypadków
5. Wymagania wobec wykonawcy: Osoba wskazana przez Wykonawcę do prowadzenia szkolenia posiada co najmniej 2-letnie doświadczenie zawodowe (praktyczne i/lub dydaktyczne) w zakresie wystąpień/szkoleń/prelekcji o tematyce bezpieczeństwa informacji. Na potwierdzenie doświadczenia Wykonawca dołączy do oferty Referencje potwierdzające realizację minimum 2 wystąpień/szkoleń/prelekcji o związanych z tematyką bezpieczeństwa informacji przeprowadzonych w okresie ostatnich 3 lat od złożenia oferty, a jeżeli ten okres jest krótszy to w tym okresie.
6. Materiały szkoleniowe: Wykonawca zobowiązany jest do przygotowania i dostarczenia uczestnikom materiałów szkoleniowych w formie drukowanej lub elektronicznej.
7. Ocena efektywności szkolenia: Po zakończeniu szkolenia, wykonawca przeprowadzi test wiedzy oraz ankietę ewaluacyjną w celu oceny efektywności szkolenia i zadowolenia uczestników.

III. Audyt SZBI, i testy podatności.

1. Przeprowadzenie pierwszego audytu wstępnego obejmującego min.:
 - a) inwentaryzację uprawnień w programach i systemach informatycznych,
 - b) inwentaryzację aktywów,
 - c) rozpoznanie struktury organizacyjnej i realizowanych procesów oraz wymagań prawnych funkcjonowania jednostki,
 - d) analiza procesów i wymagań prawnych/
2. Audyt powdrożeniowy: weryfikacja zgodności z ISO 27001, skuteczności wdrożonych kontroli i wskazanie obszarów do poprawy
3. Opracowanie raportu z rekomendacjami działań korygujących i wsparcie przy wdrażaniu poprawek
4. 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.
5. Audyt musi być przeprowadzony przez osobę posiadającą certyfikat uprawniający do przeprowadzenia audytu, o którym mowa w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.
6. Osoba skierowana do przeprowadzenia audytu zgodności wdrożonego systemu zarządzania bezpieczeństwem informacji w Gminie Urszulin musi posiadać minimum 2 letnie doświadczenie w przeprowadzaniu audytów z zakresu bezpieczeństwa informacji, potwierdzone dokumentami w postaci referencji, faktur, lub innymi dokumentami potwierdzającymi min. 2 letnie doświadczenie w realizacji zadań związanych z systemami bezpieczeństwa informacji.

IV. Testy penetracyjne infrastruktury IT i OT

Wykonawca przeprowadzi testy penetracyjne, zgodne z międzynarodowymi standardami cyberbezpieczeństwa, w tym

- a) NIST SP 800-115 - testowanie bezpieczeństwa infrastruktury IT.
- b) MITRE ATT&CK - odwzorowanie rzeczywistych technik ataków na infrastrukturę.
- c) CIS, CWE - eliminacja podatności infrastrukturalnych.
- d) OWASP - standardy dla aplikacji i systemów transakcyjnych.

obejmujące swym zakresem:

1. Analizę i skanowanie infrastruktury, w tym:
 - Automatyczne i manualne skanowanie sieci wewnętrznej oraz podsieci w celu identyfikacji dostępnych usług.
 - Analiza topologii sieci i ocena segmentacji (firewalle, VLAN/PVLAN, mechanizmy kontroli dostępu).
 - Weryfikacja segmentacji sieci LAN i jej odporności na ataki wewnętrzne.
 - Wykrywanie nieautoryzowanych urządzeń w sieci wewnętrznej.
2. Przeprowadzenie testów dostępu i kontroli uwierzytelniania, w tym:
 - Testowanie polityki dostępu i konfiguracji VPN.
 - Weryfikacje możliwości logowania do hostów poprzez interfejs webowy oraz SSH przy użyciu domyślnych poświadczeń i metod brute-force.
 - Testy kontroli dostępu do stron internetowych z poziomu urządzeń brzegowych.
3. Ocenę zabezpieczeń chmurowych i bezprzewodowych, w tym:
 - Analizę dostępnych usług chmurowych (np. AWS, Azure, Google Cloud, Oracle Cloud) pod kątem błędnych konfiguracji i narażenia na ataki.
 - Wykrywanie sieci bezprzewodowych i ocena mechanizmów zabezpieczeń.
 - Przeprowadzenie prób zakłócania działania sieci oraz wykrywanie nieautoryzowanych urządzeń.
4. Sporządzenie szczegółowego raportu opisującego podatności, ich krytyczność (CVSS), rekomendacje naprawcze i priorytety wdrożenia.
5. Raport podpisany przez certyfikowanych testerów penetracyjnych (OSCP OSWE, eWPTXv2 itp.)

V. Termin realizacji przedmiotu zamówienia

4 miesiące od dnia zawarcia umowy.

INFORMACJA KONCOWA

Wszystkie ewentualne nazwy własne i marki handlowe urządzeń i elementów zawarte w opisie przedmiotu zamówienia, zostały użyte w celu sprecyzowania oczekiwanych jakościowych i technologicznych Zamawiającego.

Zamieszczone w specyfikacji nazwy technologicznych lub producentów kluczowych komponentów użyto jedynie w celu przykładowym.

Zamawiający informuje, że dopuszcza składanie ofert, w których poszczególne urządzenia bądź materiały wymienione w opisie przedmiotu zamówienia mogą być zastąpione urządzeniami bądź materiałami/elementami równoważnymi. Poprzez pojęcie materiałów/elementów i urządzeń równoważnych należy rozumieć materiały zapewniające uzyskanie parametrów technicznych nie gorszych od założonych w opisie



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

przedmiotu zamówienia. Zastosowanie rozwiązań równoważnych nie może prowadzić do pogorszenia właściwości przedmiotu zamówienia w stosunku do przewidzianych w niniejszym zaproszeniu, ani do zmiany ceny.