Załącznik nr 1 do zapytania ofertowego

**Opis przedmiotu zamówienia**

Przedmiotem zamówienia jest opracowanie oraz wdrożenie dokumentacji wewnętrznej Systemu Zarządzania Bezpieczeństwem Informacji (dalej „SZBI”) spełniającej wymagania normy ISO/IEC 27001 oraz przeprowadzenie audytu bezpieczeństwa, jn.:

* 1. **Część 1 - Opracowanie oraz wdrożenie dokumentacji wewnętrznej Systemu Zarządzania Bezpieczeństwem Informacji (dalej „SZBI”) spełniającej wymagania normy ISO/IEC 27001;**
	2. **Część 2 - Przeprowadzenie audytu bezpieczeństwa**.

Opracowanie i wdrożenie dokumentacji SZBI oraz przeprowadzenie audytu bezpieczeństwa dotyczy trzech jednostek tj.:

* Starostwa Powiatowego w Ostródzie, około 120 pracowników, regulamin organizacyjny dostępny pod adresem https://bip.powiat.ostroda.pl/akty/6056/uchwala-w-sprawie-uchwalenia-regulaminu-organizacyjnego-starostwa-powiatowego-w-ostrodzie.html
* Powiatowego Centrum Pomocy Rodzinie w Ostródzie, około 35 pracowników, regulamin organizacyjny dostępny pod adresem https://bipspostroda.warmia.mazury.pl/akty/5991/w-sprawie-uchwalenia-regulaminu-organizacyjnego-powiatowego-centrum-pomocy-rodzinie-w-ostrodzie.html
* Zarządu Dróg Powiatowych w Ostródzie około 25 pracowników, regulamin organizacyjny dostępny pod adresem https://bip.powiat.ostroda.pl/akty/5528/w-sprawie-okreslenia-regulaminu-organizacyjnego-zarzadu-drog-powiatowych-w-ostrodzie.html

**Część 1 - Opracowanie oraz wdrożenie dokumentacji wewnętrznej Systemu Zarządzania Bezpieczeństwem Informacji (dalej „SZBI”) spełniającej wymagania normy ISO/IEC 27001**

Poprzez opracowanie dokumentacji SZBI należy rozumieć: przygotowanie przez Wykonawcę dokumentów od strony merytorycznej i formalnej spełniającej wymagania normy ISO/IEC 27001, bez podejmowania działań redakcyjnych lub innych ingerencji w treść dokumentu ze strony Zamawiającego. Opracowana dokumentacja musi być zgodna z:

* rozporządzeniem 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,
* ustawą z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (t.j. z 2024 r. poz. 1077 z późn. zm.),
* rozporządzeniem Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),
* dyrektywą Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) oraz akty wykonawcze wydane do niej

W przypadku jeżeli w okresie realizacji zamówienia zostanie przyjęta nowelizacja wyżej wymienionych przepisów prawa lub zostaną opublikowane akty wykonawcze do dyrektywy NIS2. Wykonawca ma obowiązek uwzględnić wszystkie ich wymagania przy opracowaniu i wdrażaniu dokumentacji SZBI.

Dokumentacja SZBI powinna uwzględniać i obejmować obszary takie jak:

1. Polityka bezpieczeństwa informacji:
* dokumenty i zasady,
* zobowiązania kierownictwa,
1. Organizacja bezpieczeństwa informacji:
* role i odpowiedzialność za bezpieczeństwo informacji,
* rozdzielanie obowiązków,
* bezpieczeństwo informacji w zarządzaniu projektami,
1. Zarządzanie aktywami:
* inwentaryzacja aktywów,
* użytkowania komputerów przenośnych
* postępowanie z aktywami,
* zarządzanie nośnikami wymiennymi,
* postępowanie z nośnikami danych, naprawy i likwidacja sprzętu
1. Kontrola dostępu:
	* + polityka kontroli dostępu,
		+ dostęp do sieci i usług sieciowych,
		+ rejestrowanie i wyrejestrowywanie użytkowników,
		+ nadawanie, zmiana uprawnień i dostępów oraz zarządzanie kontem,
		+ zarządzanie prawami uprzywilejowanego dostępu,
		+ zarządzanie poufnymi informacjami uwierzytelniającymi użytkowników,
		+ przegląd praw dostępu użytkowników,
		+ odbieranie lub dostosowywanie praw dostępu,
		+ stosowanie poufnych informacji uwierzytelniających,
		+ ograniczanie dostępu do informacji,
		+ procedury bezpieczeństwa logowania,
		+ system zarządzania hasłami,
		+ użycie uprzywilejowanych programów narzędziowych,
		+ zdalny dostęp,
2. Kryptografia:
	* + polityka stosowania zabezpieczeń kryptograficznych,
		+ zarządzanie kluczami,
3. Bezpieczeństwo fizyczne i środowiskowe:
	* + fizyczna granica obszaru bezpiecznego,
		+ ochrona przed zagrożeniami zewnętrznymi i środowiskowymi,
		+ praca w obszarach bezpiecznych,
		+ dostawy,
		+ lokalizacja i ochrona sprzętu,
		+ konserwacja sprzętu,
		+ bezpieczne zbywanie lub przekazywanie do ponownego użycia,
		+ polityka czystego biurka i ekranu,
		+ polityka kluczy,
4. Bezpieczna eksploatacja:
	* + dokumentowanie procedur eksploatacyjnych,
		+ rozpoczęcie, zawieszenie i zakończenie pracy w systemie,
		+ zabezpieczenia przed szkodliwym oprogramowaniem,
		+ tworzenie kopii zapasowych i archiwizacja danych,
		+ rejestrowanie zdarzeń,
		+ rejestrowanie działań administratorów i operatorów,
		+ synchronizacja zegarów,
		+ instalacja oprogramowania w systemach produkcyjnych,
		+ zarządzanie podatnościami technicznymi,
		+ ograniczenia w instalowaniu oprogramowania,
5. Bezpieczeństwo komunikacji
	* + zabezpieczenia sieci,
		+ polityki i procedury przesyłania informacji,
		+ porozumienia dotyczące przesyłania informacji,
		+ wiadomości elektroniczne,
		+ weryfikacja zapisu umów z zewnętrznymi dostawcami w celu wdrażania odpowiednich środków dla osiągnięcia celów programu cyberbezpieczeństwa,
		+ zabezpieczanie usług aplikacyjnych w sieciach publicznych,
		+ outsourcing, współpraca ze stronami trzecimi,
		1. Zarządzanie incydentami związanymi z bezpieczeństwem informacji:
		+ odpowiedzialność i procedury,
		+ zgłaszanie zdarzeń związanych z bezpieczeństwem informacji,
		+ zgłaszanie słabości związanych z bezpieczeństwem informacji,
		+ ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem,
		+ reagowanie na incydenty związane z bezpieczeństwem informacji,
		+ wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji,
		+ gromadzenie materiału dowodowego,
		+ plan reagowania na incydenty
6. Zarządzanie ciągłością działania:
* plany ciągłości działania,
* testy planów,
* odzyskiwanie po awarii.
	+ 1. Przeglądy i aktualizacja dokumentacji SZBI

W ramach usługi Wykonawca przeprowadzi analizę ryzyka dla systemu teleinformatycznego jednostek oraz opracuje dokumentację opisującej strategię zarządzania ryzykiem. Dokumentacja powinna zawierać m. in takie informacje jak:

* identyfikacja ryzyk,
* rejestr ryzyk,
* kategoryzacja ryzyk
* identyfikacja aktywów i procesów
* identyfikacja zagrożeń
* identyfikacja zabezpieczeń
* identyfikacja podatności
* szacowanie ryzyka – w tym zaproponowanie metody szacowania ryzyka
* instruktaż online dla pracowników zaangażowanych w analizę ryzyka

Wykonawca zobowiązany jest do zachowania w poufności informacji uzyskanych na etapie opracowania i wdrożenia SZBI w jednostkach na podstawie odrębnej umowy o powierzenie przetwarzania danych osobowych.

Opracowana dokumentacja zostanie przekazana Zamawiającemu w formie edytowalnych plików w formacie Word/Excel.

Dokumentacja musi zawierać wszystkie niezbędne polityki i procedury, dokumenty niezbędne do zarządzania bezpieczeństwem informacji, instrukcje, metodologie zarządzania ryzykiem, wzory wniosków, matryce itd.

Po opracowaniu i zaakceptowaniu przez Zamawiającego dokumentacji wewnętrznej SZBI Wykonawca przeprowadzi w formie zdalnej instruktaż dla pracowników jednostek w celu zaznajomienia ich z zapisami SZBI. Wykonawca przekaże Zamawiającemu nagranie z przeprowadzonego instruktażu.

**Część 2 - Przeprowadzenie audytu bezpieczeństwa**

Po zakończeniu przez Zamawiającego realizacji wszystkich zadań objętych projektem[[1]](#footnote-1), Wykonawca w okresie 02.01.2026r.-20.02.2026r., zrealizuje usługę polegającą na przeprowadzeniu audytu cyberbezpieczeństwa w jednostkach: Starostwo Powiatowe w Ostródzie, Powiatowe Centrum Pomocy Rodzinie w Ostródzie oraz Zarząd Dróg Powiatowych w Ostródzie zgodnie z zakresem określonym w Regulaminie Konkursu Grantowego „Cyberbezpieczny Samorząd stanowiącym załącznik nr 2 do umowy.

Wykonawca dostarczy Zamawiającemu raport z audytu (opis zakresu przeprowadzonych prac audytowych, analizę informacji zebranych podczas audytów, wnioski i zalecenia związane z rozwiązaniem występujących problemów). Powyższe dokumenty należy przygotować oddzielnie dla każdej jednostki.

Wykonawca udzieli wsparcia merytorycznego dla każdej jednostki przy wypełnianiu ankiety dojrzałości cyberbezpieczeństwa (załącznik nr 6 do Regulaminu Konkursu Grantowego „Cyberbezpieczny Samorząd”), stanowiącej załącznik nr 3 do umowy. Wstępnie wypełniona ankieta (stan obecny i planowany) zostanie udostępniona Wykonawcy po podpisaniu umowy.

**Dotyczy części 1 i 2:**

Wykonawca upoważni Zamawiającego do korzystania z dokumentacji powstałej w związku z realizacją przedmiotu zamówienia bez ograniczeń czasowych i terytorialnych, na wszystkich znanych polach eksploatacji, w szczególności w zakresie:

1. utrwalania i zwielokrotniania w dowolnej formie i technice;
2. wprowadzania do obrotu, użyczania, najmu lub udostępniania osobom trzecim w całości lub części;
3. publicznego rozpowszechniania, w tym w Internecie;
4. przetwarzania w celu realizacji Projektu;
5. wykorzystania w celu promocji Projektu;
6. dokonywania zmian, modyfikacji, adaptacji, tłumaczenia oraz tworzenia opracowań, a także korzystania z takich opracowań;
7. przekazywania praw określonych w punktach powyżej osobom trzecim.

Wynagrodzenie Wykonawcy obejmuje upoważnienie do korzystania z dokumentacji w wyżej wskazanym zakresie. Wykonawca oświadczy, że dokumentacja nie naruszają praw osób trzecich.

1. „Cyberbezpieczny Samorząd”, dofinansowanego w formie grantu z programu Fundusze Europejskie na Rozwój Cyfrowy 2021 – 2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa. [↑](#footnote-ref-1)