*Załącznik nr 1 do zaproszenia do składania ofert*

**Opis przedmiotu zamówienia**

**pn.: Opracowanie i wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji oraz wykonanie audytu powdrożeniowego w ramach projektu „Podniesienie poziomu cyberbezpieczeństwa w Starostwie Powiatowym w Lubaczowie”**.

Przedmiotem zamówienia jest zlecenie opracowania oraz wdrożenia dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w Starostwie Powiatowym w Lubaczowie (dalej „SZBI”), spełniającej wymagania normy ISO/IEC 27001 oraz przeprowadzenie audytu wdrożonego systemu bezpieczeństwa informacji w ramach projektu „Podniesienie poziomu cyberbezpieczeństwa w Starostwie Powiatowym w Lubaczowie”, realizowanego w ramach Konkursu Grantowego „Cyberbezpieczny Samorząd” współfinansowanego przez Unię Europejską w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa. Umowa o powierzenie grantu z dnia 24.06.2024 r. o numerze FERC.02.02-CS.01-001/23/1407/FERC.02.02-CS.01-001/23/2024.

Zamawiający przewiduje w ramach przedmiotu zamówienia dwa etapy realizacji:

1) **Etap 1 - Opracowanie oraz wdrożenie dokumentacji wewnętrznej Systemu Zarządzania Bezpieczeństwem Informacji spełniającej wymagania normy PN ISO/IEC 27001;**

2) **Etap 2 - Przeprowadzenie audytu wdrożonego systemu bezpieczeństwa informacji.**

Opracowanie i wdrożenie dokumentacji SZBI oraz przeprowadzenie audytu dotyczy Starostwa Powiatowego w Lubaczowie ul. Jasna 1, 37-600 Lubaczów. Jednostka zatrudnia około 75 pracowników, regulamin organizacyjny dostępny pod adresem: https://bip.powiatlubaczowski.pl/383,1-status-prawny-i-organizacja.

**<u>Etap 1 - Opracowanie oraz wdrożenie dokumentacji wewnętrznej Systemu Zarządzania Bezpieczeństwem Informacji spełniającej wymagania normy PN ISO/IEC 27001.</u>**

Poprzez opracowanie dokumentacji SZBI należy rozumieć: przygotowanie przez Wykonawcę projektów dokumentów spełniających wymagania normy PN ISO/IEC 27001, które po uzgodnieniu

z Zamawiającym zostaną dostosowane do specyfiki jego działalności. 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 aktami wykonawczymi wydanymi 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,
2) Organizacja bezpieczeństwa informacji:
   - role i odpowiedzialność za bezpieczeństwo informacji,
   - rozdzielanie obowiązków,
   - bezpieczeństwo informacji w zarządzaniu projektami,
3) Zarządzanie aktywami:
   - inwentaryzacja aktywów,
   - użytkowania komputerów przenośnych
   - postępowanie z aktywami,
   - zarządzanie nośnikami wymiennymi,
   - postępowanie z nośnikami danych, naprawy i likwidacja sprzętu

4) 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,
5) Kryptografia:
   - polityka stosowania zabezpieczeń kryptograficznych,
   - zarządzanie kluczami,
6) 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,
7) 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,

8) 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,
9) 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
10) Zarządzanie ciągłością działania:
   - plany ciągłości działania,
   - testy planów,
   - odzyskiwanie po awarii.
11) Przeglądy i aktualizacja dokumentacji SZBI

W ramach usługi Wykonawca przeprowadzi analizę ryzyka dla systemów teleinformatycznych w Starostwie Powiatowym w Lubaczowie oraz opracuje dokumentację opisującą 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 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 Starostwa w celu zaznajomienia ich z zapisami SZBI. Wykonawca przekaże Zamawiającemu nagranie z przeprowadzonego instruktażu.

**Etap 2 - Przeprowadzenie audytu wdrożonego systemu bezpieczeństwa informacji**.

Po zakończeniu przez Zamawiającego realizacji wszystkich zadań objętych projektem[1], Wykonawca w okresie 01.06.2026 r. – 12.06.2026 r., zrealizuje usługę polegającą na przeprowadzeniu audytu wdrożonego systemu bezpieczeństwa informacji w Starostwie Powiatowym w Lubaczowie, zgodnie z zakresem określonym w Regulaminie Konkursu Grantowego „Cyberbezpieczny Samorząd", dostępnym pod adresem: https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad.

Wykonawca dostarczy Zamawiającemu raport z audytu (opis zakresu przeprowadzonych prac audytowych, analizę informacji zebranych podczas audytów, wnioski i zalecenia związane z rozwiązaniem występujących problemów).

Wykonawca udzieli wsparcia merytorycznego przy wypełnianiu ankiety dojrzałości cyberbezpieczeństwa (załącznik nr 6 do Regulaminu Konkursu Grantowego „Cyberbezpieczny

[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.

Samorząd"). Wstępnie wypełniona ankieta (stan obecny i planowany) zostanie udostępniona Wykonawcy po podpisaniu umowy.

**Dotyczy etapu 1 i 2:**

Wykonawca upoważni Zamawiającego do korzystania z dokumentacji powstałej w związku 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 narusza praw osób trzecich.

**Termin realizacji przedmiotu zamówienia:**

1) Etap 1: od dnia podpisania umowy do 31.05.2026 r.;
2) Etap 2: w okresie 01.06.2026 r. – 12.06.2026 r.

**Warunki udziału w postępowaniu:**

O udzielenie zamówienia mogą ubiegać się wykonawcy, którzy spełniają warunki udziału w postępowaniu, dotyczące zdolności technicznej lub zawodowej, tj.:

1) Wykonawca w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres działalności jest krótszy, w tym okresie, opracował i wdrożył dokumentację SZBI (lub dokonał jej dostosowania do aktualnych wymogów prawnych) w co najmniej dwóch jednostkach administracji publicznej.
2) Wykonawca dysponuje osobą zdolną do realizacji przedmiotu zamówienia w zakresie etapu 2, tj. osobą, której zamierza powierzyć pełnienie funkcji audytora. Wskazana osoba musi posiadać co najmniej:

a) 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) lub będącego audytorem zewnętrznym systemu zarządzania bezpieczeństwem informacji według normy PN ISO/IEC 27001 oraz
b) min. 2 letnie doświadczenie zawodowe w charakterze audytora bezpieczeństwa.