Urząd Gminy Koszęcin
ul. Powstańców Śl. 10 42-286 Koszęcin

E-mail: koszecin@koszecin.pl
Tel.: 34 3576 100 • Fax.: 34 3576 108

Załącznik nr 2
do zaproszenia do składania ofert
z dnia 09 października 2025 r.
nr IZ.7011.20.2025

OPIS PRZEDMIOTU ZAMÓWIENIA

Dla zadania pn.

„Opracowanie, przegląd i aktualizacja i wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy Koszęcin"

1. Opracowany i wdrożony System Zarządzania Bezpieczeństwem Informacji („SZBI") musi uwzględniać wymagania:
   1) Rozporządzenia Rady Ministrów z dnia 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 („KRI");
   2) Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa w zakresie w jakim dotyczy podmiotów publicznych nie świadczących usług kluczowych („UoKSC")
   3) Rozporządzenia 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;
   4) Ustawy o ochronie danych osobowych z dnia 10 maja 2018 r.
   5) Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2005 nr 64 poz. 565); Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000); Przepisami dziedzinowymi prawa UE i/lub krajowego określającego dla Zamawiającego wymagania w zakresie bezpieczeństwa informacji;
   6) wymagania Polskiej aktualnej wersji Normy PN ISO/IEC 27001, PN-ISO/IEC 20000, dobrych praktyk w dziedzinie cyberbezpieczeństwa
2. Opracowanie/aktualizacja SZBI nie dotyczy informacji niejawnych w rozumieniu przepisów ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2018 r. poz. 412, z późn. zm.6).
3. Etapy wdrożenia SZBI obejmą w szczególności:
   a) analizę obecnie funkcjonującej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.
   b) opracowanie rekomendacji zabezpieczeń.
   c) opracowanie i wdrożenie polityk, procedur, instrukcji SZBI.
   d) opracowanie planów ciągłości działania, planów awaryjnych.
   e) integracja (zapewnienie zgodności SZBI) z funkcjonującym w Urzędzie Systemem Kontroli Zarządczej.
   f) opracowanie projektu zarządzenia w sprawie wdrożenia SZBI.

g) szkolenie dla kadry zarządzającej w zakresie wdrożenia SZBI.
h) szkolenie dla pracowników w zakresie wdrożenia SZBI.

Etap 1 „Analiza"
W ramach etapu Wykonawca przeprowadzi następujące czynności

1) Analizę obecnie funkcjonującego Systemu Zarządzania Bezpieczeństwem Informacji w tym kontekstu Zamawiającego w szczególności:
   a) struktura organizacyjna;
   b) role i kompetencje osób odpowiedzialnych za zarządzanie bezpieczeństwem informacji
   c) obieg informacji w ramach SZBI
   d) systemy informatyczne własne, powierzone w drodze umowy, porozumień, przepisu prawa;
   e) zweryfikuje obecnie stosowane zabezpieczenia fizyczne oraz techniczne stosowane przez Zamawiającego
   f) wyspecyfikuje ryzyka jakie zostały zidentyfikowane podczas realizacji etapu „Analiza"
2) Sporządzi sprawozdanie z wykonania audytu obecnie funkcjonującego SZBI, w którym m.in wyspecyfikuje; zakres rekomendowanych zmian w zakresie istniejącej SZBI w tym zalecanych/rekomendowanych zabezpieczeń fizycznych, organizacyjnych i technicznych. Wykonawca przekaże sprawozdanie w formie pliku pdf
3) Przedstawi koncepcję aktualizacji i wdrożenia SZBI

Etap II – Opracowanie/aktualizacja SZBI

1) Na podstawie uzgodnień poczynionych pomiędzy Zamawiającym a Wykonawcą w związku z przekazanym sprawozdaniem z wykonania audytu obecnie funkcjonującego SZBI, Wykonawca opracuje projekt SZBI dostosowany do uzgodnionych i przyjętych wymagań Zamawiającego.
2) Opracowany projekt SZBI nie jest dokumentem wiążącym dla Zamawiającego, może on podlegać modyfikacjom na skutek wzajemnych uzgodnień. Zamawiający zastrzega sobie prawo do wnoszenia uwag na każdym etapie realizacji przedmiotu zamówienia.

Etap III. Wdrożenie i szkolenia

1) Wykonawca opracuje materiały szkoleniowe w związku z wdrożeniem zaktualizowanego SZBI.
2) Wykonawca przeprowadzi szkolenia trwające m.in. 2 godziny każde dla: Kadry kierowniczej Zamawiającego, osób pozostałych pracowników, których zakres SZBI w jakimkolwiek stopniu dotyczy.
3) Szkolenie zostaną przeprowadzone w formie stacjonarnej w siedzibie Zamawiającego w terminach uzgodnionych z Wykonawcą.

Etap IV – Wsparcie w eksploatacji SZBI

1) Wykonawca zapewni aktualizację SZBI w okresie 2 lat po zakończeniu realizacji zadania.

I. Wymagania wobec wykonawcy

1. Zamawiający wymaga aby Wykonawca wykazał wykonanie co najmniej 3 wdrożeń SZBI dla jednostek sektora finansów publicznych
2. Co najmniej jednym wdrożeniem systemu kontroli zarządczej dla Jednostki samorządu

terytorialnego

3. Zamawiający wymaga aby Wykonawca oddelegował do realizacji zadania co najmniej:
   1) 2 audytorów, z których każdy z nich posiadaj aktualne certyfikaty potwierdzające wiedzę ekspercką z zakresu zarządzania systemem bezpieczeństwa informacji oraz zarządzania ciągłością działania:
      a) audytora wiodącego norm: PN-EN ISO/IEC 27001
      b) audytora wiodącego norm: PN-EN ISO/IEC 22301
   2) Eksperta ds. cyberbezpieczeństwa o uprawnieniach audytora wiodącego norm: PN-EN ISO/IEC 27001 posiadającego udokumentowane doświadczenie w pełnieniu funkcji kierowniczej (kierownik/dyrektor) komórki organizacyjnej odpowiedzialnej za zarządzanie cyberbezpieczeństwem w podmiocie posiadającym aktualny certyfikat na zgodność z normą ISO/IEC 27001 lub ISO/IEC 22301.
   3) Eksperta ds. zarządzania usługami IT o uprawnieniach audytora wiodącego normy ISO/IEC 20000.

   Zamawiający wyłącza możliwość powoływania się na zasoby podmiotów trzecich lub możliwość podzlecenia wykonania usługi. Zamawiający nie dopuszcza formy zdalnej przeprowadzenia przedmiotu zamówienia.