Załącznik nr 2 do WZ 7/2025

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Opracowanie nowych polityk i aktualizacja dokumentacji w ramach opracowania i wdrożenia SZBI wraz z analizą ryzyka w Urzędzie.
   a) Etap 1 - Wykonanie analizy wstępnej posiadanego Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy w Bądkowie:
      - obszary działalności Zamawiającego i realizowanych zadań,
      - strukturę organizacyjną Zamawiającego,
      - specyfikę pracy poszczególnych referatów organizacyjnych Zamawiającego,
      - systemy informatyczne użytkowane przez Zamawiającego,
      - rejestry publiczne pozostające we właściwości Zamawiającego,
      - SZBI aktualnie funkcjonujący u Zamawiającego,
      - wstępną identyfikację informacji przetwarzanych u Zamawiającego,
      - wstępną identyfikację ryzyk związanych z utratą poufności, integralności i dostępności informacji przetwarzanych u Zamawiającego.

      Analiza musi być zakończona przedstawieniem raportu pozwalającego stwierdzić Zamawiającemu, na jakim poziomie jest zarządzanie bezpieczeństwem informacji oraz jakie obszary powinien jeszcze doskonalić, aby osiągnąć gotowość do wdrożenia dobrych praktyk w oparciu o normę ISO 27001, rozporządzenie KRI oraz ustawie o Krajowym Systemie Cyberbezpieczeństwa. Analiza umożliwi określenie struktury dokumentacji nowego SZBI, która powinna mieć układ hierarchiczny, tj. opisywać nowy SZBI na różnych poziomach szczegółowości oraz określać zagadnienia, które muszą zostać obligatoryjnie uregulowane.

   b) Etap 2 - Opracowanie Systemu Zarządzania Bezpieczeństwem Informacji wraz z Analizą Ryzyka dla Urzędu Gminy w Bądkowie. Stworzony SZBI powinien być zgodny z rozporządzeniem KRI i spełniać wymagania normy PN-ISO/IEC 27001, w tym obejmować następujące obszary mające wpływ na bezpieczeństwo w organizacji Zamawiającego:
      - Polityka Bezpieczeństwa,
      - Organizacja bezpieczeństwa informacji,
      - Bezpieczeństwo zasobów ludzkich,
      - Zarządzanie aktywami,
      - Kontrola dostępu,
      - Kryptografia,
      - Bezpieczeństwo fizyczne i środowiskowe,
      - Bezpieczna eksploatacja,
      - Bezpieczna komunikacja,
      - Pozyskiwanie, rozwój i utrzymanie systemów,
      - Relacje z dostawcami,

- Zarządzanie incydentami związanymi z bezpieczeństwem informacji,
- Aspekty bezpieczeństwa w zarządzaniu ciągłością działania,
- Zgodność z wymaganiami prawnymi i własnymi standardami.

Stworzony SZBI musi być zgodny z aktualnymi przepisami powszechnie obowiązującego prawa, w tym w szczególności z przepisami:

- rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2024 r. poz. 773);
- 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1);
- ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781);
- ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2024 r. poz. 307);
- ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2022 r. poz. 902);
- ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz.U. z 2024 r. poz. 632);
- ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2024 r. poz. 1077);
- dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii.
- oraz uwzględniać wewnętrzne akty prawne obowiązujące u Zamawiającego.

W ramach opracowania nowego SZBI Wykonawca między innymi:

- zaproponuje obszary funkcjonalne, które powinny zostać objęte nowym SZBI, spójne z treścią raportu z etapu I zaakceptowanego przez Zamawiającego;
- uwzględni w szczególności następujące zagadnienia:
  - określenie organizacji bezpieczeństwa informacji,
  - identyfikacja aktywów informacyjnych i klasyfikacja informacji przetwarzanych u Zamawiającego,
  - szacowanie ryzyka oraz postępowanie z ryzykiem, związanych z utratą poufności, integralności i dostępności informacji przetwarzanych u Zamawiającego,
  - bezpieczeństwo w procesach zarządzania zasobami ludzkimi,

- kontrola dostępu,
- zasady nadawania uprawnień,
- zasady tworzenia i zmiany haseł,
- polityka czystego biurka i ekranu,
- bezpieczeństwo fizyczne i środowiskowe,
- klasyfikacja informacji,
- odpowiedzialność za zasoby,
- postępowanie z nośnikami informacji,
- użytkowanie urządzeń mobilnych i praca zdalna,
- zarządzanie sprzętem informatycznym,
- instalacja oprogramowania,
- ochrona przed złośliwym oprogramowaniem,
- kopie zapasowe,
- zarządzanie zmianami, w szczególności w systemach informatycznych oraz infrastrukturze informatycznej,
- zarządzanie dokumentacją infrastruktury informatycznej,
- monitorowanie systemów informatycznych,
- zarządzanie pojemnością,
- serwis i konserwacja infrastruktury informatycznej,
- zarządzanie podatnościami technicznymi,
- zarządzanie incydentami bezpieczeństwa,
- zabezpieczenia kryptograficzne,
- bezpieczeństwo sieci i transmisji danych,
- ochrona własności intelektualnej,
- bezpieczeństwo informacji w relacjach z dostawcami,
- ciągłość działania,
- zasady bezpieczeństwa informacji w procesach pozyskiwania, rozwoju i utrzymania systemów informacyjnych,
- weryfikacja zgodności z wymaganiami prawnymi,
- korzystanie z poczty elektronicznej i Internetu,
- zarządzanie usługami informatycznymi,
- utrzymanie i doskonalenie SZBI,
- przeprowadzanie audytów SZBI.

W/w zagadnienia zostaną dopasowane do urzędu oraz wewnętrznych regulacji i rozwiązań. Po przeprowadzonej analizie ryzyka, zostanie udostępnione narzędzie oraz metodyka do samodzielnej analizy.

Wymagania dotyczące spotkań projektowych: Liczba spotkań projektowych wynosi minimum 2-3 udokumentowane spotkania z kadrą kierowniczą. Spotkania te mają na celu zebranie informacji niezbędnych do opracowania indywidualnych procedur oraz omówienie specyficznych potrzeb i wymagań.

2. Przeprowadzenie szkoleń z zakresu bezpieczeństwa informacji dla pracowników Urzędu w siedzibie zamawiającego oddzielnie**:**
   a) dla kadry zarządzającej Urzędu,
   b) dla pozostałych pracowników Urzędu.

   Szkolenia muszą obejmować m.in.:
   a) wymogi wynikające z KRI, UoKSC i RODO,
   b) zarządzanie ryzykiem w bezpieczeństwie informacji,
   c) System Zarzadzania Bezpieczeństwem informacji – jak skutecznie przestrzegać procedur wdrożonej Polityki Bezpieczeństwa Informacji,
   d) ciągłość działania – dlaczego jest istotna i jak ją wdrożyć,
   e) identyfikowanie zagrożeń – jak wdrożyć odpowiednie rozwiązania na przestrzeganie zasad bezpieczeństwa
   f) przegląd znanych typów ataków na JST - najnowsze zagrożenia.

3. Szkolenia z zakresu cyberbezpieczeństwa dla pracowników Urzędu w siedzibie zamawiającego oddzielnie:
   a) dla kadry zarządzającej Urzędu,
   b) dla pozostałych pracowników Urzędu.

   Szkolenia muszą obejmować m.in.:
   a) podstawy prawne i główne zasady cyberbezpieczeństwa,
   b) bezpieczeństwo informacji – podstawowe wiadomości, z uwzględnieniem regulacji wewnętrznych oraz wymagań rozporządzenia KRI:
      - wewnętrzne procedury w obszarze bezpieczeństwa informacji cyberbezpieczeństwa,
      - wymagania dla pracowników wynikające z KRI, UoKSC oraz RODO
      - System Zarządzania Bezpieczeństwem Informacji w praktyce,
   c) przegląd najpopularniejszych zagrożeń i zasady bezpiecznego korzystania z internetu:
      - ochrona informacji i prywatność w internecie,
      - ransomware jako poważne zagrożenie dla JST,
      - phishing, oszustwa i wyłudzenia z uwzględnieniem oszustwa typu BEC (Business E-mail Compromise)
      - Cyberhigiena, w tym bezpieczeństwo urządzeń i bezpieczeństwo fizyczne
      - bezpieczne hasła i uwierzytelnienie dwuskładnikowe
      - wewnętrzne zalecenia i rekomendacje, w tym sposoby reakcji na incydenty bezpieczeństwa.

Wykonawca zobowiązuje się do wykonania niniejszej usługi za pomocą własnych zasobów.