Usługa opracowania dokumentacji oraz wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Chociwlu, z wyłączeniem analizy ryzyka, audytu wewnętrznego, szkoleń i wsparcia doradczego

1. Przedmiot zamówienia
Przedmiotem zamówienia jest usługa polegająca na **opracowaniu dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji oraz wdrożeniu SZBI w Urzędzie Miejskim w Chociwlu**, z wyłączeniem usług analizy ryzyka, audytu wewnętrznego, szkoleń oraz bieżącego wsparcia doradczego, realizowanych odrębnie na rzecz Zamawiającego.

2. Opis przedmiotu zamówienia
Przedmiot zamówienia obejmuje usługę polegającą na opracowaniu dokumentacji oraz wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Chociwlu, w szczególności w zakresie:
2.1
Opracowania projektu zarządzenia wdrażającego SZBI i Politykę Bezpieczeństwa Informacji w Urzędzie Miejskim w Chociwlu.
2.2
Opracowania od podstaw dokumentacji SZBI, zgodnej co najmniej z:
- normą ISO/IEC 27001,
- Rozporządzeniem Rady Ministrów w sprawie Krajowych Ram Interoperacyjności,
- ustawą o krajowym systemie cyberbezpieczeństwa,
- wymaganiami programu „Cyberbezpieczny Samorząd”.

2.3
Opracowanie dokumentacji obejmującej co najmniej:
- Politykę Bezpieczeństwa Informacji,
- politykę zarządzania dostępem oraz uprawnieniami do systemów informacyjnych,
- procedurę nadawania, zmiany i odbierania uprawnień,
- zasady stosowania haseł oraz uwierzytelniania użytkowników,
- procedurę reagowania na incydenty bezpieczeństwa informacji,
- procedurę zgłaszania, rejestrowania, obsługi i analizy incydentów,
- procedurę tworzenia kopii zapasowych oraz odtwarzania danych,
- procedurę testowania kopii zapasowych i odtwarzania danych,
- procedurę zarządzania ciągłością działania w zakresie wymaganym dla Zamawiającego,
- procedurę postępowania w przypadku awarii, niedostępności systemów lub utraty danych,
- zasady użytkowania sprzętu służbowego, oprogramowania oraz nośników informacji,
- zasady bezpiecznej pracy na stacjach roboczych,
- zasady bezpiecznego korzystania z poczty elektronicznej oraz Internetu,
- zasady pracy zdalnej,
- zasady ochrony urządzeń mobilnych,
- zasady klasyfikacji informacji i postępowania z informacjami,
- zasady ochrony danych wrażliwych oraz danych osobowych w zakresie związanym z SZBI,
- zasady zarządzania aktywami informacyjnymi,

- rejestr aktywów informacyjnych, opracowany na potrzeby dokumentacji SZBI i wdrożenia, z uwzględnieniem danych oraz ustaleń przekazanych przez Zamawiającego i podmiot realizujący analizę ryzyka na podstawie odrębnej umowy
- zasady zarządzania podatnościami i aktualizacjami bezpieczeństwa,
- zasady zarządzania zmianą w środowisku IT w zakresie wpływającym na bezpieczeństwo informacji,
- zasady prowadzenia i przechowywania logów oraz monitorowania zdarzeń bezpieczeństwa,
- zasady bezpieczeństwa fizycznego i środowiskowego w zakresie adekwatnym do warunków Zamawiającego,
- zasady współpracy z podmiotami zewnętrznymi i dostawcami usług w zakresie bezpieczeństwa informacji,
- zasady przeglądu, aktualizacji oraz nadzoru nad dokumentacją SZBI,
- zasady przeprowadzania okresowych przeglądów zarządczych SZBI,
- rejestr incydentów bezpieczeństwa informacji,
- wykaz ról i odpowiedzialności w obszarze bezpieczeństwa informacji,
- wzory niezbędnych formularzy, rejestrów, upoważnień, oświadczeń i protokołów związanych z funkcjonowaniem SZBI,
- inne dokumenty, procedury, instrukcje i rejestry niezbędne do prawidłowego wdrożenia, utrzymania i funkcjonowania SZBI u Zamawiającego,
- Opracowanie Deklaracji Stosowania (Statement of Applicability) zgodnej z ISO/IEC 27001, zawierającej wykaz zabezpieczeń właściwych dla Zamawiającego, uzasadnienie ich zastosowania albo wyłączenia oraz odniesienie do dokumentacji SZBI i wdrożonych rozwiązań organizacyjnych.

Dokumentacja ma tworzyć spójny i kompletny system dokumentów umożliwiający wdrożenie, utrzymanie, nadzorowanie i doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji u Zamawiającego, zgodnie z wymaganiami normy ISO/IEC 27001, Krajowych Ram Interoperacyjności, ustawy o krajowym systemie cyberbezpieczeństwa oraz wymogami programu „Cyberbezpieczny Samorząd”.

2.4

Uwzględnienia w opracowywanej dokumentacji zaleceń wskazanych przez Audytora Wiodącego ISO/IEC 27001 współpracującego z Zamawiającym na podstawie odrębnej umowy oraz zaleceń wynikających z audytu KRI przeprowadzonego w październiku 2025 r.

2.5

Przekazania opracowanej dokumentacji w formacie PDF oraz w wersji edytowalnej.

2.6

Wdrożenie SZBI w warstwie organizacyjnej, w tym wdrożenie rozwiązań wynikających z opracowanej dokumentacji, obejmuje co najmniej:

- wdrożenie zasad i procedur bezpieczeństwa informacji do stosowania w Urzędzie,
- określenie ról, odpowiedzialności i zasad nadzoru w ramach SZBI,
- wdrożenie zasad zarządzania dostępem i uprawnieniami,
- wdrożenie zasad zgłaszania, rejestrowania i obsługi incydentów bezpieczeństwa informacji,
- wdrożenie zasad wykonywania kopii zapasowych i odtwarzania danych,

- wdrożenie zasad postępowania z aktywami informacyjnymi oraz nośnikami danych,
- wdrożenie zasad klasyfikacji i ochrony informacji,
- wdrożenie zasad bezpiecznego korzystania ze sprzętu, oprogramowania, poczty elektronicznej i Internetu,
- wdrożenie zasad przeglądu, aktualizacji i nadzoru nad dokumentacją SZBI,
- przygotowanie Zamawiającego do stosowania przyjętych rozwiązań organizacyjnych w bieżącej działalności.

2.7
Współpraca z podmiotem świadczącym na rzecz Zamawiającego usługi doradcze i audytowe w zakresie bezpieczeństwa informacji, wyłącznie w zakresie niezbędnym do zapewnienia zgodności opracowywanej dokumentacji i działań wdrożeniowych z wynikami analizy ryzyka, zaleceniami audytowymi oraz przyjętymi założeniami SZBI.
2.8

Przekazanie dokumentacji powdrożeniowej obejmującej co najmniej:

- opis wdrożonych rozwiązań organizacyjnych i technicznych,
- opis wdrożonych procedur i mechanizmów bezpieczeństwa,
- opis konfiguracji i ustawień wdrożonych rozwiązań,
- opis sposobu działania i współzależności wdrożonych elementów SZBI,
- zasady administrowania, utrzymania i bieżącej eksploatacji wdrożonych rozwiązań,
- zasady wykonywania czynności kontrolnych, przeglądowych i aktualizacyjnych,
- zasady wykonywania kopii zapasowych oraz odtwarzania danych,
- zasady zarządzania uprawnieniami i dostępami,
- instrukcje postępowania w przypadku awarii, incydentu bezpieczeństwa lub utraty dostępności,
- wykaz dokumentów, rejestrów, formularzy i instrukcji przekazanych Zamawiającemu,
- zalecenia dotyczące dalszego utrzymania, przeglądu i doskonalenia SZBI.

2.9 Zakres niniejszego zamówienia nie obejmuje:

1. przeprowadzenia analizy ryzyka,
2. opracowania metodyki oceny ryzyka,
3. sporządzenia rejestru ryzyk oraz planu postępowania z ryzykiem,
4. przeprowadzenia audytu wewnętrznego bezpieczeństwa informacji,
5. przeprowadzenia szkoleń pracowników,
6. bieżącego wsparcia doradczego, konsultacyjnego i operacyjnego w okresie obowiązywania SZBI, ponieważ zadania te realizowane są przez inny podmiot na podstawie odrębnej umowy.