



Cyberbezpieczny Samorząd

Załącznik nr 2 do Zapytania ofertowego

Opis przedmiotu zamówienia

Przedmiotem zamówienia jest opracowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji, zwanego dalej SZBI oraz szkolenie wszystkich pracowników i kierownictwa Urzędu Miejskiego w Oławie w zakresie wymagań SZBI.

1. Kod CPV 79417000-0: Usługi doradcze w zakresie bezpieczeństwa
80550000-4: Usługi szkolenia w dziedzinie bezpieczeństwa
72810000-1: Usługi audytu komputerowego
79131000-1 Usługi w zakresie dokumentów
2. Przedmiotem zamówienia jest **Opracowanie dokumentacji SZBI, przeprowadzenie audytu SZBI oraz szkolenie wszystkich pracowników i kierownictwa urzędu w zakresie wymagań SZBI, w podziale na zadania:**

Zadanie nr 1: Opracowania dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji:

Minimalny zakres prac:

ETAP I. Audyt zerowy - diagnoza przedwdrożeniowa – prace wykonane w siedzibie urzędu w wymiarze minimum 2 dni roboczych

- analiza dokumentacji urzędu, zapoznanie się z dostępnymi regulacjami wewnętrznymi mającymi wpływ na bezpieczeństwo informacji.
- przeprowadzenie przez wykonawcę audytu w organizacji, w tym:
 - a) wywiady z kluczowymi pracownikami, piastującymi funkcje istotne z perspektywy bezpieczeństwa informacji ,
 - b) weryfikacja zgodności dokumentacji oraz procedur z normą ISO 27001,
 - c) identyfikacja i analiza luk w organizacji pod kątem zapewnienia bezpieczeństwa informacji oraz spełniania wymagań normy ISO 27001.
- opracowanie wyników audytu.
- opracowanie raportu wraz propozycją planu realizacji kolejnych etapów.

ETAP II. Analiza ryzyka - prace wykonane w siedzibie urzędu w wymiarze minimum 2 dni roboczych

- przedstawienie propozycji metodyki analizy ryzyka w ramach Systemu Zarządzania Bezpieczeństwem Informacji.
- przeprowadzenie inwentaryzacji aktywów związanych z przetwarzaniem informacji oraz ich klasyfikacja uwzględniając specyfikę organizacji.
- przeprowadzenie analizy ryzyka w ramach SZBI, przy wsparciu wykonawcy.
- opracowanie raportu zbiorczego, tj. podsumowania zrealizowanych prac i wynikających z tego wniosków.

ETAP III. Opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji - prace wykonane w siedzibie urzędu w wymiarze minimum 2 dni roboczych

- Polityki bezpieczeństwa informacji
- Polityki ochrony danych osobowych
- Zasady bezpieczeństwa teleinformatycznego
- Zasady bezpieczeństwa osobowego
- Zasady bezpieczeństwa prawno-organizacyjnego
- Zasady bezpieczeństwa fizycznego
- Inne niezbędne i wymagane dokumenty (instrukcje, regulaminy)

ETAP IV. Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji - prace wykonane w siedzibie urzędu w wymiarze minimum 2 dni roboczych

- przygotowanie materiałów szkoleniowych dla pracowników.
- wsparcie przy przeprowadzeniu audytu wewnętrznego w ramach SZBI.
- wsparcie przy przeprowadzeniu przeglądu zarządzania w organizacji.

Dokumentacja SZBI musi zawierać wszystkie elementy określone w obowiązującej wersji norm ISO/IEC 27001 i ISO/IEC 27005, oraz zawierać politykę ochrony danych osobowych zgodną z RODO.

Opracowanie dokumentacji SZBI ma być zgodne z:

- normami ISO/IEC 27001, ISO 22301,



Fundusze Europejskie
na Rozwój Cyfrowy

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

- 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 (Dz. U. poz. 773),
- Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2023 r. poz. 913 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) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.),
- Dyrektywa 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) (Dz. U. UE. L. z 2022 r. Nr 333, str. 80)

Zadanie nr 2: Przeprowadzenie audytu wdrożonego SZBI według normy ISO/IEC 27001.

Audyt musi zostać przeprowadzony w okresie do 6 miesięcy od opracowania dokumentacji SZBI.

Audyt musi zostać przeprowadzony w siedzibie zamawiającego w wymierz minimum 2 dni roboczych.

Audyt musi być wykonany przez audytorów posiadających uprawnienia i doświadczenie opisane szczegółowo w pkt V. przedmiotowego Zapytania – „V. WYMAGANIA DOTYCZĄCE PRZEDMIOTU ZAMÓWIENIA”.

Zadanie nr 3: Przeprowadzenie szkolenia wszystkich pracowników i kierownictwa urzędu w zakresie wymagań SZBI.

Szkolenie musi omówić cały zakres opracowanej w zadaniu nr 1 dokumentacji SZBI.

Szkolenie musi zostać przeprowadzone stacjonarnie z podziałem na minimum dwie grupy dla wszystkich pracowników i minimum jedną grupę dla kierownictwa urzędu. Czas trwania szkolenia minimum 4h na jedną grupę uczestników.

3. Informacje dodatkowe.

Zamawiający informuje, że Urząd Miejski w Oławie zatrudnionych jest 100 pracowników, którzy realizują zadania w lokalizacjach:

- a) Plac Zamkowy 15, 55-200 Oława (główna siedziba Urzędu),
- b) Ul. Rynek 1, 55-200 Oława (drugi budynek Urzędu),
- c) ul. Młyńska 12, 55-200 Oława (wydział Profilaktyki Uzależnień),
- d) ul. Rynek 25, 55-200 Oława (Urząd Stanu Cywilnego)



Fundusze Europejskie
na Rozwój Cyfrowy

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA