



GMINA I MIASTO PYZDRY

Pyzdry, 26 czerwca 2025 r.

OR.FZ.042.8.2024

Zapytanie ofertowe

Zamówienie o wartości szacunkowej nieprzekraczającej równowartości 130 000 złotych, wyłączone z obowiązku stosowania przepisów ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U. z 2024 r. poz. 1320 ze zm.)

Burmistrz Pyzdr zwraca się z prośbą o przygotowanie oferty na stworzenie i wdrożenie dokumentacji systemu zarządzania bezpieczeństwem informacji (SZBI) zgodnie z normą ISO/IEC 27001

1. Przedmiot zamówienia

Zamówienie polega na stworzeniu i wdrożeniu dokumentacji systemu zarządzania bezpieczeństwem informacji (SZBI) w Urzędzie Miejskim w Pyzdrach zgodnie z normą ISO/IEC 27001 w ramach projektu „Cyberbezpieczny samorząd”. Projekt realizowany w ramach Konkursu Grantowego „Cyberbezpieczny Samorząd” (Priorytet II: Zaawansowane usługi cyfrowe. Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa Fundusze Europejskie na Rozwój Cyfrowy 2021-2027).

2. Przedmiot zamówienia:

Przedmiotem zamówienia jest stworzenie i wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnie z normą ISO/IEC 27001. System powinien uwzględniać wymagania postulowane w aktach prawnych:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE". Rozporządzenie to zostało opublikowane w Dzienniku Urzędowym Unii Europejskiej L 119 z 4 maja 2016 roku,
- Rozporządzenie 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. 2024 poz. 773)
- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tj. Dz.U. 2024 poz. 1077) z uwzględnieniem projektu nowelizacji wdrażającej Dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148

Dokumentacja powinna obejmować następujące elementy postulowane przez sekcje wymagań normy ISO/IEC 27001 i/lub kontroli zawartych w załączniku A normy:

- Organizacja Systemu Zarządzania Bezpieczeństwem Informacji: Definicja struktury oraz przypisanie odpowiedzialności za zarządzanie bezpieczeństwem informacji w urzędzie.
- Zakres i granice SZBI: Określenie obszarów działalności, które są objęte systemem, w tym zasoby, procesy oraz informacyjne granice.



GMINA I MIASTO PYZDRY

- Identyfikacja wymagań interesariuszy: Określenie sposobu identyfikowania wymagań ustawowych, normatywnych i umownych i uwzględniania ich w SZBI
- Polityka bezpieczeństwa informacji: Dokument określający fundamentalne zasady oraz cele dotyczące ochrony informacji w urzędzie.
- Cele bezpieczeństwa informacji: Ustalenie precyzyjnych celów, które organizacja chce zrealizować w zakresie bezpieczeństwa informacji.
- Metodyka szacowania ryzyka i postępowania z ryzykiem: Ustanowienie sposobu szacowania ryzyka oraz zarządzania nim.
- Deklaracja stosowania: Określenie które kontrole załącznika A normy będą stosowane.
- Szkolenia i uświadomienie: Programy edukacyjne dla pracowników, mające na celu zwiększenie świadomości dotyczącej zagrożeń związanych z bezpieczeństwem informacji.
- Nadzorowanie dokumentacji: Procedury przeglądania oraz aktualizacji dokumentacji SZBI, zapewniające, że wszystkie informacje są na bieżąco aktualizowane.
- Audyty wewnętrzne: Harmonogram oraz procedury przeprowadzania audytów w celu weryfikacji efektywności oraz zgodności SZBI.
- Działania korygujące: Mechanizmy identyfikacji, analizy i usuwania niezgodności w funkcjonowaniu SZBI.
- Przegląd zarządzania: Regularne przeglądy realizacji i skuteczności SZBI, które będą prowadzone przez kierownictwo urzędowe.
- Strategia dotycząca zasobów: Zasady zarządzania zasobami ludzkimi, technologicznymi oraz materialnymi, niezbędnymi dla efektywności SZBI.
- Bezpieczeństwo w zarządzaniu projektami: Wytyczne dotyczące integracji aspektów bezpieczeństwa w projektach realizowanych w urzędzie.
- Polityka korzystania z urządzeń mobilnych: Zasady użycia oraz zabezpieczeń dotyczących urządzeń mobilnych wykorzystywanych przez pracowników.
- Telepraca: Regulacje dotyczące pracy zdalnej, w tym zabezpieczenia związane z dostępem do informacji.
- Warunki zatrudnienia: Zasady zatrudniania odnoszące się do aspektów bezpieczeństwa informacji.
- Postępowanie z nośnikami: Procedury zarządzania nośnikami danych oraz ich bezpiecznego przechowywania.
- Polityka kontroli dostępu: Zasady regulujące dostęp do danych i systemów informacyjnych.
- Polityka bezpieczeństwa fizycznego i środowiskowego: Zabezpieczenia fizyczne mające na celu ochronę danych i informacji. Praca w strefach bezpieczeństwa
- Zabezpieczenie pomieszczeń i obiektów: Procedury sformalizowane dotyczące ochrony przestrzeni, w których są przechowywane informacje.
- Polityka czystego biurka i ekranu: Zasady dotyczące porządku w miejscu pracy oraz ochrony informacji.
- Polityka kopii zapasowych: Procedury dotyczące tworzenia, przechowywania i zarządzania kopiami zapasowymi danych.
- Polityka ochrony logów: Zasady dotyczące zarządzania informacjami zapisanymi w logach systemowych.
- Zarządzanie podatnościami technicznymi: Procedury identyfikacji podatności w systemach IT oraz ich eliminacji.



GMINA I MIASTO PYZDRY

- Bezpieczeństwo komunikacji: Regulacje dotyczące ochrony informacji w komunikacji wewnętrznej oraz zewnętrznej.
- Ogólna strategia ciągłości działania i polityka ciągłości działania.
- Audyty wewnętrzne: Polityki i procedury realizacji audytów.
- Przeglądy zarządzania: Procedura i dokumenty.

UWAGA! Dokumentacja ma uwzględniać kontekst, strukturę, wymagania ustawowe zamawiającego, a więc wymaga dokładnego przeanalizowania wszelkich procesów zamawiającego mających wpływ na bezpieczeństwo informacji.

Prace wdrożeniowe polegać mają na pełnym uruchomieniu systemu: ogłoszeniu systemu, określeniu wymagań prawnych, branżowych, umownych i innych, zidentyfikowaniu aktywów informacyjnych oraz ich klasyfikacji, dokonaniu analizy ryzyka z uwzględnieniem zagrożeń dla aktywów wspomagających, zarządzaniu ryzykiem, wyborze zabezpieczeń i stworzeniu deklaracji stosowania, przeprowadzeniu pierwszego audytu wewnętrznego bezpieczeństwa informacji, przeprowadzeniu przeglądu zarządzania oraz określeniu niezbędnych działań korygujących, planu ich wdrożenia i kontroli wykonania.

Realizacja usługi wymaga obecności w Urzędzie na etapie tworzenia SZBI oraz podczas wdrażania.

3. Wymogi dla oferentów biorących udział w postępowaniu:

- Posiadanie certyfikatu audytora wiodącego normy ISO 27001 nieprzerwanie przynajmniej od 4 lat.
- Posiadanie wykształcenia (studia magisterskie lub podyplomowe) w zakresie cyberbezpieczeństwa lub ochrony danych osobowych lub informatycznego lub pokrewnego.
- Posiadanie doświadczenia we współpracy z administracją publiczną w realizacji należycie wykonanych usług w prowadzeniu i wdrażaniu projektów z zakresu cyberbezpieczeństwa oraz opracowania i wdrożenia SZBI od 2020 roku.

Na potwierdzenie powyższych wymogów oferent przedstawi dokumenty potwierdzające posiadanie certyfikatu, wykształcenia oraz doświadczenia. Niespełnienie któregośkolwiek z wymogów skutkować będzie odrzuceniem oferty.

4. Termin realizacji:

Termin dostarczenia dokumentacji: **4 miesiące od podpisania umowy, wdrożenie do 31.05.2026 r.**

5. Kryteria oceny ofert:

- Cena 100%

Jeżeli zostały złożone oferty o takiej samej cenie. Zamawiający wezwie oferentów, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych. Oferenci składający oferty dodatkowe nie mogą zaoferować cen wyższych niż zaoferowane w złożonych ofertach.



GMINA I MIASTO PYZDRY

6. Opis sposobu przygotowania oferty:

Oferta powinna:

- posiadać datę sporządzenia
- zawierać adres lub siedzibę oferenta, numer telefonu, NIP
- zawierać proponowaną cenę netto lub brutto.

7. Miejsce oraz termin składania ofert:

Ofertę należy złożyć **do dnia 4 lipca 2025 r. do godz. 15.00** elektronicznie na adres e-mail: admin@pyzdry.pl, lub pisemnie na adres: Urząd Miejski w Pyzdrach, ul. Taczanowskiego 1, 62-310 Pyzdry, biuro nr 13. Oferty złożone po terminie oraz oferty, których treść nie odpowiada treści zapytania ofertowego nie będą rozpatrywane.

8. Określenie warunków dokonywania zmian umowy:

Zamawiający dopuszcza możliwość zmian umowy. Zmiany mogą dotyczyć w szczególności:

- zmiany powszechnie obowiązujących przepisów prawa w zakresie mającym wpływ na realizację przedmiotu zamówienia lub świadczenia stron,
- zmiany stawki podatku VAT,
- zmian dotyczących sposobu płatności.

Wszelkie istotne zmiany w umowie wymagają formy pisemnej pod rygorem nieważności.

9. Sposób rozliczenia

Po wykonaniu przedmiotu zamówienia zapłata dokonana będzie przelewem na rachunek bankowy Wykonawcy, wskazany w wystawionej przez Wykonawcę fakturze VAT, w terminie do 21 dni od wystawienia faktury.

10. Uwagi

Zamawiający dopuszcza możliwości powierzenia części lub całości zamówienia podwykonawcom. Zamówienie nie może być udzielane podmiotom powiązanym z Zamawiającym osobowo lub kapitałowo.

11. Dodatkowe informacje:

Dodatkowych informacji w sprawie zamówienia udziela Pani Grażyna Juszcak tel. 63-2768-333, wew. 110.

Przemysław Dębski

/-/ Burmistrz Pyzdr