Załącznik nr 1 do zapytania ofertowego

OPIS PRZEDMIOTU ZAMÓWIENIA

dot. zadania pn. **„Wykonanie Audytów i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji "**

Zamówienie obejmuje obszar organizacyjny w ramach projektu „**Cyberbezpieczny Samorząd w Gminie Gzy”.**
Przedmiotem zamówienia jest Wykonanie audytu przedwdrożeniowego, opracowanie i wdrożenie wspólnej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz wykonanie audytu powdrożeniowego dla Gminy Gzy według najnowszej obowiązującej polskiej normy PN EN ISO/IEC 27001:2023 w ramach konkursu grantowego "Cyberbezpieczny Samorząd".
Przedmiotem zamówienia objęte są jednostki: **Gmina Gzy**

Zamawiający przewiduje w ramach przedmiotu zamówienia następujące etapy realizacji:

I. Wykonanie audytu przedwdrożeniowego.

KONTEKST, ZAŁOŻENIA DOTYCZĄCE ZAMÓWIENIA

1. Celem zamówienia jest podniesienie poziomu bezpieczeństwa przetwarzanych informacji oraz systemów informatycznych Zamawiającego poprzez określenie do wdrożenia niezbędnych elementów Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z wymaganiami ujętymi w: ISO/IEC 27001:2022 (PN-ISO/IEC 27001:2023), PN- ISO/IEC 27005:2022, PN-ISO/IEC 22301:2020 wynikających z przepisów prawa dla jednostek wskazanych powyżej:
2. Informacje ogólne o środowisku Zamawiającego:
   a) Przetwarzanie informacji odbywa się według wskazanej wcześniej listy jednostek. Informacje przetwarzane są w formie papierowej oraz systemach informatycznych. Zamawiający zatrudnia około 30 osób.
   b) Środowisko teleinformatyczne zawiera obecnie około 5 elementów aktywnych sieci, 4 serwerów fizycznych, 4 serwerów wirtualnych, zlokalizowanych w jednostkach wskazanych w liście powyżej.
3. Zamawiający w ciągu 14 dni kalendarzowych od dnia zawarcia Umowy przekaże Wykonawcy dokumenty, którymi dysponuje w obszarze związanym z bezpieczeństwem informacji, w tym procedury wewnętrzne i wyniki przeprowadzonych audytów oraz szczegółową strukturę organizacyjną i informacje o środowisku teleinformatycznym, niezbędne do opracowania przez Wykonawcę wstępnego harmonogramu prac.

ZAKRES ZAMÓWIENIA

Usługa będzie obejmować swoim zakresem:

- audyt przedwdrożeniowy u Zamawiającego;
- audyt bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usług kluczowych

Audyt przedwdrożeniowy

Audyt przedwdrożeniowy ma na celu weryfikację poziomu spełnienia wymagań normy PN-ISO/IEC 27001:2023 przez Zamawiającego, w tym ocenę skuteczności zabezpieczeń technicznych, organizacyjnych

i prawnych stosowanych u Zamawiającego, w wszystkich obszarach określonych załącznikiem A do ww. normy.

4. **Audyt bezpieczeństwa systemów informacyjnych**

Przeprowadzenie audytu bezpieczeństwa w oparciu o wymagania załącznika A do normy ISO 27001 oraz wytycznych normy ISO 27002 w zakresie bezpieczeństwa systemów informatycznych wykorzystywanych do świadczenia usług dla klientów jednostek.

Audyt powinien zawierać także wskazania podatności systemów informatycznych: wskazanie podatności, wagi podatności, opis podatności, informacje dotyczące podatności w tym źródła zewnętrzne, rekomendacje co do sposobu postępowania

Wykonawca przy wykonywaniu umowy może oprócz audytorów wskazanych powyżej dodatkowo posiłkować się innymi pracownikami i współpracownikami Wykonawcy.

Powierzenie wykonania części przedmiotu Umowy innym pracownikom i współpracownikom nie wymaga uprzedniej zgody Zamawiającego, przy czym Wykonawca odpowiada za działania osób trzecich jak za działania własne.

Po zakończeniu audytu Wykonawca przygotuje i przekaże w formie elektronicznej oraz papierowej sprawozdanie z przeprowadzonego audytu.

Ogólne wymagania odnośnie do audytu.

Audyty: (łączny czas trwania audytu nie krótszy niż 16 godziny robocze)

- Audyt Techniczny – wymagań zawartych w załączniku A normy ISO/IEC 27001
- Audyt Systemowy – wymagań normy zawartych normie ISO/IEC 27001
- Sporządzenie raportów w formie pisemnej (edytowalnej i nieedytowalnej)
- Przekazanie raportów do klienta
- Wykonanie, razem z klientem, działań po audytowych w formie uzgodnionej z klientem. Jeżeli występuje konieczność korekty dokumentacji, wykonuje ją Wykonawca.

II. <u>Opracowanie i wdrożenie Systemu zarządzania Bezpieczeństwem Informacji zgodnie z normą PN-EN ISO/IEC 27001;</u>

Opracowanie przez Wykonawcę niżej wymienionych dokumentów, przygotowanie przez Wykonawcę dokumentów od strony merytorycznej i formalnej do stanu, który pozwala przekazać dokumenty jednostce certyfikującej, bez podejmowania działań redakcyjnych lub innych ingerencji w treść dokumentu ze strony Zamawiającego. Po stronie Zamawiającego leży jedynie uzgodnienie treści dokumentów z Wykonawcą.

Klasyfikacja informacji przetwarzanych u Zamawiającego

W ramach procesu klasyfikacji informacji Wykonawca jest zobowiązany do zrealizowania następujących prac:

- opracowanie metodyki klasyfikowania informacji przetwarzanych u Zamawiającego;
- opracowanie modelu podziału informacji przetwarzanych u Zamawiającego w zależności od poziomu ich wrażliwości i przeznaczenia;
- sklasyfikowanie wspólnie z pracownikami poszczególnych komórek organizacyjnych informacji przetwarzanych u Zamawiającego;

- opracowanie raportu z procesu klasyfikacji informacji.

Szacowanie ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych u Zamawiającego zgodnie z wytycznymi normy PN-ISO/IEC 27005:2022

W ramach usługi Wykonawca jest zobowiązany przeprowadzić proces szacowania ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych u Zamawiającego, a w szczególności:

- opracować metodykę szacowania ryzyka spełniającą wymagania PN-ISO/IEC 27005:2022, optymalną ze względu na charakter działalności Zamawiającego;
- opracować kryteria akceptacji ryzyka i określić akceptowane poziomy ryzyk;
- przeprowadzić wspólnie z wyznaczonymi pracownikami Zamawiającego proces szacowania ryzyka, w tym:
    - zinwentaryzować zasoby (aktywa informacyjne) oraz ich właścicieli, określić zagrożenia dla zasobów, określić podatności dla zasobów, określić skutki utraty poufności, integralności i dostępności zasobów oraz przeanalizować i ocenić zidentyfikowane ryzyka;
    - opracować raport z procesu szacowania ryzyka, uwzględniający wszystkie zidentyfikowane ryzyka utraty poufności, integralności i dostępności informacji Zamawiającego;
    - opracować przy współudziale wyznaczonych pracowników Zamawiającego plan postępowania z ryzykiem.

Opracowanie dokumentów niezbędnych do wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji

Opracowanie wraz z przekazaniem praw autorskich dokumentów niezbędnych do opracowania systemu zarządzania bezpieczeństwem informacji zgodnie z wymaganiami:

a) ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne
b) rozporządzenia 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
c) ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa.

Wykonawca, na podstawie wyników uzyskanych w trakcie realizacji audytu przedwdrożeniowego, procesu klasyfikacji informacji oraz szacowania ryzyka, zobowiązany jest przedstawić elementy niezbędne do uzupełniania w celu opracowania dokumentacji SZBI przez Zamawiającego a także wytypować procesy niezbędne do poprawnego funkcjonowania organizacji. Dokument/y muszą ponadto stanowić szczegółowy wykaz dokumentów niezbędnych do opracowania na potrzeby SZBI z zaznaczeniem ich wzajemnych powiązań, w tym:

- Dokument Główny Polityki Zarządzania Bezpieczeństwa Informacji definiujący m.in. jej cele, zakres, wymogi prawne ochrony informacji, deklarację zaangażowania najwyższego kierownictwa, procesy, wykaz informacji chronionych, role i odpowiedzialności w zakresie bezpieczeństwa informacji;
- Deklarację Stosowania wraz z odniesieniem do obecnie opracowywanych dokumentów
- Polityki bezpieczeństwa dla poszczególnych obszarów funkcjonalnych bezpieczeństwa informacji u Zamawiającego w tym dla obszaru: teleinformatycznego, spraw osobowych, zabezpieczeń

fizycznych, ciągłości działania, definiujących podstawowe wymagania bezpieczeństwa i ochrony informacji, a także procedury i instrukcje stanowiące zestaw szczegółowych dokumentów, wynikających z tych polityk bezpieczeństwa;

- Regulaminy definiujące prawa i obowiązki pracowników w zakresie bezpieczeństwa informacji.

Wykonawca gwarantuje, że dokumentacja systemu zarządzania bezpieczeństwem informacji jest zgodna z wymaganiami normy ISO/IEC 27001 oraz wymaganiami certyfikacyjnymi jednostki certyfikującej systemy zarządzania na zgodność z normą ISO/IEC 27001, akredytowanej przez Polską jednostkę akredytującą wymienioną na stronie http://www.iaf.nu//articles/IAF_MEMBERS_SIGNATORIES/4.

1. Zakres systemu zarządzania bezpieczeństwem informacji
2. Księga systemu zarządzania bezpieczeństwem informacji
3. Polityka bezpieczeństwa informacji
4. Schemat organizacyjny kierowania sprawami bezpieczeństwa informacji
5. Mapa procesów objętych SZBI minimum 6 procesów (min. proces zarzadzania i utrzymania SZBI, proces zarządzania ryzykiem, proces zarzadzania incydentami (RODO, UoKSC), proces zarządzania dostawami (wybór-realizacja-zakończenie współpracy), proces zarzadzania pracownikami (rekrutacja-zatrudnienie-zwolnienie), proces obsługi interesanta (obsługa wniosków). Schemat procesów należy przygotować w notacji BPMN (forma edytowalna)
6. Deklaracja stosowania dla systemu bezpieczeństwa informacji wraz z przyporządkowanie aktualnie używanych w organizacji rozwiązań do wymagań normy.
7. Plan kontynuacji działania (BCP) zgodny z wymaganiami określonymi w normie ISO22301:2019
8. Metodyka szacowania ryzyka zgodnie z wymaganiami normy ISO27005:2022
9. Wszystkie procedury potrzebne do przejścia procesu certyfikacji:
    - Procedura nadzoru nad dokumentami
    - Procedura działań korekcyjnych, korygujących i zapobiegawczych
    - Procedura audytu wewnętrznego
    - Procedura nadzoru nad zapisami
    - Procedura przeglądu zarządzania
    - Procedura zarządzania incydentami
    - Procedura bezpieczeństwa wewnętrznego organizacji
    - Procedura ewakuacji personelu i sprzętu z obiektów
    - Procedura klasyfikacji informacji wewnętrznych i zewnętrznych
    - Procedura oceny ryzyk generowanych przez strony zewnętrzne (klientów, dostawców, kooperantów, innych)
    - Procedura postępowania w przypadku odejścia pracownika z firmy
    - Procedura bezpieczeństwa infrastruktury teleinformatycznej (sieć, serwerownie, urządzenia łączności, inne elementy)
    - Procedura bezpieczeństwa fizycznego
    - Procedura nadzór nad przyrządami pomiarowymi i zapewnienia spójności pomiarowej
    - Inne niezbędne u Zamawiającego z punktu widzenia systemu bezpieczeństwa informacji (po ocenie potrzeb)
        - Dokumenty ustalające status systemu zarządzania bezpieczeństwem informacji zgodnie z wymaganiami normy.
        - Opracowanie formularzy i rejestrów będących integralną częścią w/w dokumentów w formie i treści odpowiedniej do potrzeb i woli klienta (zawartość merytoryczna oraz forma).
10. Analiza ryzyk u Zamawiającego zgodnie z wymaganiami normy ISO27005:2022
    - Identyfikacja aktywów
    - Identyfikacja i ocena podatności, które mogą być wykorzystane przez zagrożenia dla aktywów

- Identyfikacja i ocena skutków utraty poufności, integralności i dostępności w odniesieniu do aktywów
- Ocena ryzyka

11. Analiza ryzyk u Zamawiającego zgodnie z wymaganiami normy ISO222301(BIA)
12. Zapoznanie pracowników Zamawiającego z wymaganiami z zakresu: (łączny czas trwania nie krótszy niż 8 godzin roboczych)
    - -normy ISO/IEC 27001
    - -załącznika A normy ISO/IEC 27001
    - szacowania ryzyka dla organizacji, dla konkretnych ryzyk, z podaniem wzorów i obliczeń
    - Podstaw prawnych dla w/w systemu
13. Wdrożenie dokumentów do stosowania, a w szczególności:
    - Przygotowanie i przekazanie wytycznych odnośnie do elektronicznego nadzorowania dokumentów i zapisów, jeżeli potrzebne, konfiguracja ustawień
    - Uzupełnienia zapisów wymaganych normą razem z Zamawiającym
    - Konsultacje indywidualne z zakresu stosowania opracowanej dokumentacji
    - Udzielenie wszelkiego wsparcia w celu uzyskania biegłego posługiwania się przez Zamawiającego systemem (nie miej niż 20 godzin)

III. Wykonanie audytu powdrożeniowego w zakresie spełnienia wymagań opracowania i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji, zgodnie z wymaganiami normy PN-ISO/IEC 27001:2023

I. KONTEKST, ZAŁOŻENIA DOTYCZĄCE ZAMÓWIENIA

1. Celem zamówienia jest sprawdzenie poziomu bezpieczeństwa przetwarzanych informacji oraz systemów informatycznych Zamawiającego w zakresie spełnienia wymagań opracowania i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji, zgodnie z wymaganiami norm ujętymi w: ISO/IEC 27001:2022 (PN-ISO/IEC 27001:2023), PN- ISO/IEC 27005:2022, PN-ISO/IEC 22301:2019 wynikających z przepisów prawa dla jednostek wskazanych powyżej:
2. Informacje ogólne o środowisku Zamawiającego:
   a) Przetwarzanie informacji odbywa się według wskazanej wcześniej listy jednostek. Informacje przetwarzane są w formie papierowej oraz systemach informatycznych. Zamawiający zatrudnia około 30 osób.
   b) Środowisko teleinformatyczne zawiera obecnie około 5 elementów aktywnych sieci, 4 serwery fizyczne, 4 serwery wirtualne, zlokalizowanych w jednostkach wskazanych w liście powyżej.
3. Zamawiający przekaże Wykonawcy dokumenty, którymi dysponuje w obszarze związanym z bezpieczeństwem informacji, w tym procedury wewnętrzne i wyniki przeprowadzonych audytów oraz szczegółową strukturę organizacyjną i informacje o środowisku teleinformatycznym, niezbędne do opracowania przez Wykonawcę wstępnego harmonogramu prac.

ZAKRES ZAMÓWIENIA

Usługa będzie obejmować swoim zakresem:

- audyt powdrożeniowy SZBI Zamawiającego;
- audyt bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usług przez listę jednostek wymienionych powyżej
- audyt systemów informacyjnych wykorzystywanych przez Zamawiającego we wskazanych w liście powyżej lokalizacjach.

Audyt ma na celu weryfikację poziomu spełnienia wymagań normy PN-ISO/IEC 27001:2022 przez Zamawiającego, w tym ocenę skuteczności zabezpieczeń technicznych, organizacyjnych i prawnych stosowanych u Zamawiającego, w wszystkich obszarach określonych załącznikiem A do ww. normy.

- **Audyt bezpieczeństwa systemów informacyjnych**

Przeprowadzenie audytu bezpieczeństwa w oparciu o wymagania załącznika A do normy ISO27001 oraz wytycznych normy ISO27002 w zakresie bezpieczeństwa systemów informatycznych wykorzystywanych do świadczenia usług dla klientów jednostek.

Audyt powinien zawierać także wskazania podatności systemów informatycznych: wskazanie podatności, wagi podatności, opis podatności, informacje dotyczące podatności w tym źródła zewnętrzne, rekomendacje co do sposobu postępowania.

Wykonawca przy wykonywaniu umowy może oprócz audytorów dodatkowo posiłkować się innymi pracownikami i współpracownikami Wykonawcy.

Powierzenie wykonania części przedmiotu Umowy innym pracownikom i współpracownikom nie wymaga uprzedniej zgody Zamawiającego, przy czym Wykonawca odpowiada za działania osób trzecich jak za działania własne.

Po zakończeniu audytu Wykonawca przygotuje i przekaże w formie elektronicznej oraz papierowej sprawozdanie z przeprowadzonego audytu.

Podpisane elektronicznie przez Tomasz Sobieraj (Certyfikat kwalifikowany) w dniu 2025-04-24.

Signed by / Podpisano przez:
Sławomir Janusz Stachura
Date / Data: 2025-04-24 13:17