Załącznik nr 2 do zapytania ofertowego

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest opracowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji, zwanego dalej SZBI zgodnie z obowiązującą normą ISO w Starostwie Powiatowym w Sokołowie Podlaskim

Wykonawca musi zrealizować usługę polegającą na przeprowadzeniu audytu cyberbezpieczeństwa w Starostwie Powiatowym w Sokołowie Podlaskim ramach projektu „Cyberbezpieczny samorząd" zgodnie z zakresem oraz formularzem stanowiącym załącznik nr 6 do Regulaminu Konkursu Grantowego „Cyberbezpieczny samorząd" zakończonego raportem oraz opracowanie dokumentacji SZBI w oparciu o KRI/KSC i normę ISO27001. Wykonanie i przekazanie Raportu z Audytu (opis zakresu przeprowadzonych prac audytowych, analizę informacji zebranych podczas audytów, wnioski i zalecenia związane z rozwiązaniem występujących problemów, analiza złożonego zał. nr 6 konkursu grantowego).

Zamawiający przewiduje w ramach przedmiotu zamówienia następujące etapy realizacji:

1) analiza działalności Zamawiającego i sporządzenie audytu przedwdrożeniowego;
2) opracowanie SZBI zgodnie z normą PN-EN ISO/IEC 27001 i przeprowadzenie szkoleń dla kadry kierowniczej i pracowników;
3) świadczenie asysty podczas wdrażania dokumentacji;
4) opracowanie audytu powdrożeniowego i ankiety.

W celu przeprowadzenia analizy Zamawiający udostępni Wykonawcy niezbędne dokumenty. Dokumenty niezbędne do opracowani audytu udostępniane będą przez Zamawiającego jedynie w jego siedzibie. Dokumenty nie będą udostępniane elektronicznie przez Zamawiającego.

Ad. 1

1. Identyfikacja i opis ustanowionych procesów w organizacji oraz ich interakcji (podejście procesowe do zarządzania bezpieczeństwem informacji zgodnie z ISO/IEC 27001:2023)
2. Zdefiniowanie kryteriów procesów.
3. Przeprowadzenie identyfikacji zasobów informacyjnych przetwarzanych przez organizację oraz sposobów zabezpieczenia informacji oraz odpowiedzialności.
4. Identyfikacja aktywów informacyjnych i ich właścicieli w kontekście procesów ustanowionych w organizacji.

Po przeanalizowaniu działalności Zamawiającego Wykonawca opracuje sprawozdanie, w którym zaproponuje koncepcję poprawy cyberbezpieczeństwa urzędu i zakres SZBI.

Ad.2

1. W ramach II etapu Wykonawca na podstawie przedstawionych sprawozdań i analiz, które zostaną zaakceptowane przez Zamawiającego, opracuje SZBI, które będzie dostosowane do potrzeb Zamawiającego. Nowy SZBI będzie zgodny z przepisami prawa, które są powszechnie obowiązujące.
2. Wraz z projektem SZBI wykonawca przedstawi zestawienie, w którym wykaże spełnienie przez SZBI wymagań dotyczących bezpieczeństwa informacji wynikających z aktualnych przepisów powszechnie obowiązującego prawa, w tym rozporządzenia KRI, a także odpowiednich norm. Zestawienie zostanie przekazane Zamawiającemu w formie elektronicznej.

3. Zamawiający zastrzega sobie prawo wnoszenia uwag do zaproponowanego SZBI, w tym do rodzaju dokumentów, zakresu merytorycznego itp.

Dokumentacja zostanie opracowana zgodnie z następującym zakresem:

Wykonawca gwarantuje, że opracowana przez niego dokumentacja systemu zarządzania bezpieczeństwem informacji będzie 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 klienta 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 klienta 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. Audyty: (łączny czas trwania audytu nie krótszy niż 16 godzin roboczych)
    - Audyt Techniczny – wymagań zawartych w załączniku A normy ISO/IEC 27001
    - Audyt Systemowy – wymagań normy zawartych normie ISO/IEC 27001
    - Audyt Ciągłości Działania – wymagań normy zawartych normie ISO/IEC 22301
    - Sporządzenie raportów w formie pisemnej (edytowalnej i nieedytowalnej
    - Przekazanie raportów do klienta
    - Wykonanie, razem z klientem, działań poaudytowych w formie uzgodnionej z klientem. Jeżeli występuje konieczność korekty dokumentacji, wykonuje ją Wykonawca

4. Wykonawca zaproponuje szkolenia wdrażające system SZBI.

Podczas wdrażania powinny odbyć się co najmniej 2 szkolenia stacjonarne, trwające co najmniej 5 godzin każde. Szkolenia powinny objąć kadrę kierowniczą Zamawiającego oraz pracowników odpowiedzialnych za funkcjonowanie SZBI w urzędzie.

Szkolenia zorganizowane zostaną w siedzibie Zamawiającego.

Zakres merytoryczny zostanie uzgodniony z Zamawiającym po przedstawieniu przez Wykonawcę projektu SZBI.

Wykonawca zobowiązuje się do przekazania Zamawiającemu materiałów szkoleniowych niezbędnych do przeprowadzenia szkoleń i wydania wszystkim uczestnikom zaświadczeń uczestnictwa w szkoleniu.

Ad. 3

Wykonawca będzie świadczył usługę asysty w następującym zakresie:

1) przygotowania i przekazania wytycznych odnośnie elektronicznego nadzorowania dokumentów i zapisów, jeżeli potrzebne, konfiguracja ustawień
2) uzupełniania zapisów wymaganych normą razem z klientem
3) praktyczne szkolenie w formie konsultacji indywidualnych z zakresu stosowania opracowanej dokumentacji
4) udzielanie wszelkiego wsparcia w celu uzyskania biegłego posługiwania się przez klienta systemem (nie miej niż 20 godzin).

Usługi asysty mogą być świadczone zdalnie lub w siedzibie Zamawiającego. Decyzja co do formy świadczenia asysty zależeć będzie każdorazowo od charakteru sytuacji.

Ad. 4

Wykonawca opracuje audyt powdrożeniowy, który będzie miał na celu przedstawienie Zamawiającemu postęp prac jaki został zrealizowany podczas wdrażania SZBI.
Usługa będzie obejmować swoim zakresem:

1) audyt powdrożeniowy SZBI Zamawiającego;
2) audyt bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej

1. Audyt

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.

2. **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 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 papierowe sprawozdanie z przeprowadzonego audytu i naniesie dane do ankiety wskazanej w załączniku nr 6 do regulaminu konkursu