Załącznik nr 2 do zapytania ofertowego

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Przedmiotem zamówienia jest opracowanie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) wraz z przeprowadzeniem audytu wdrożonego systemu zarządzania bezpieczeństwem informacji - Gmina Kije.

Wykonawca musi zrealizować usługę polegającą na przeprowadzeniu audytu cyberbezpieczeństwa w 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 oraz zapisów dostosowanych do Dyrektywy NIS2. 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 i przeprowadzenie instruktaży 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.

**Uwaga: Dokumenty niezbędne do opracowania audytu udostępniane będą przez Zamawiającego jedynie w jego siedzibie. Dokumenty nie będą udostępniane elektronicznie przez Zamawiającego.**

# Etap 1: analiza działalności Zamawiającego i sporządzenie audytu przedwdrożeniowego

1. Identyfikacja i opis ustanowionych procesów w organizacji oraz ich interakcji (podejście procesowe do zarządzania bezpieczeństwem informacji)
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.

# Etap 2: opracowanie SZBI i przeprowadzenie instruktaży dla kadry kierowniczej i pracowników

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. 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 w oparciu o wymagania normy ISO/IEC 27001.

Minimalny zakres systemu zarządzania bezpieczeństwem informacji:

* 1. Księga systemu zarządzania bezpieczeństwem informacji
  2. Polityka bezpieczeństwa informacji
  3. Schemat organizacyjny kierowania sprawami bezpieczeństwa informacji
  4. Mapa procesów objętych SZBI minimum 6 procesów (min. proces zarządzania i utrzymania SZBI, proces zarządzania ryzykiem, proces zarządzania incydentami (RODO, UoKSC), proces zarządzania dostawami (wybór-realizacja-zakończenie współpracy), proces zarządzania pracownikami (rekrutacja-zatrudnienie-zwolnienie), proces obsługi interesanta (obsługa wniosków). Schemat procesów należy przygotować w notacji BPMN (forma edytowalna).
  5. Deklaracja stosowania dla systemu bezpieczeństwa informacji wraz z przyporządkowaniem aktualnie używanych w organizacji rozwiązań do wymagań.
  6. Plan ciągłości działania (BCP)
  7. Metodyka szacowania ryzyka
  8. Procedury:
     + 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 organizacji
     + Procedura bezpieczeństwa infrastruktury teleinformatycznej (sieć, serwerownie, urządzenia łączności, inne elementy)
     + Procedura bezpieczeństwa fizycznego
     + Inne niezbędne u klienta z punktu widzenia systemu bezpieczeństwa informacji (po ocenie potrzeb)
  9. Dokumenty ustalające status systemu zarządzania bezpieczeństwem informacji.
  10. Opracowanie formularzy i rejestrów będących integralną częścią ww. dokumentów w formie i treści odpowiedniej do potrzeb i woli klienta (zawartość merytoryczna oraz forma).
  11. Analiza ryzyk:
  + 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
  1. Audyty: (łączny czas trwania audytu nie krótszy niż 16 godzin roboczych)
  + Audyt Techniczny
  + Audyt Systemowy
  + Audyt Ciągłości Działania
  + Sporządzenie raportów w formie pisemnej (edytowalnej i nieedytowalnej)
  + Przekazanie raportów
  + Wykonanie, razem z zamawiającym działań poaudytowych w uzgodnionej formie.

Jeżeli wystąpi konieczność korekty dokumentacji, wykonuje ją Wykonawca

1. Wykonawca zaproponuje instruktaże wdrażające system SZBI.

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

Instruktaże zorganizowane zostaną w siedzibie Zamawiającego.

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

Wykonawca zobowiązuje się do przekazania Zamawiającemu materiałów niezbędnych do przeprowadzenia instruktaży i wydania wszystkim uczestnikom zaświadczeń uczestnictwa.

# Etap 3: świadczenie asysty podczas wdrażania dokumentacji

Wykonawca będzie świadczył usługę asysty w następującym zakresie:

1. przygotowania i przekazania wytycznych odnośnie elektronicznego nadzorowania dokumentów
2. uzupełniania zapisów w dokumentach razem z Zamawiającym
3. praktyczne instruktaże w formie konsultacji indywidualnych z zakresu stosowania opracowanej dokumentacji
4. udzielanie wszelkiego wsparcia w celu uzyskania biegłego posługiwania się przez Zamawiającego systemem (nie mniej 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.

# Etap 4: opracowanie audytu powdrożeniowego i ankiety

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: Audyt ma na celu weryfikację poziomu spełnienia wymagań prawnych przez Zamawiającego, w tym ocenę skuteczności zabezpieczeń technicznych, organizacyjnych i prawnych stosowanych u Zamawiającego.
2. 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