

Załącznik nr 2 do SWZ

Przeprowadzenie audytów wraz ze szkoleniami

Wymagania Ogólne

I. Przegląd i aktualizacja dokumentacji PBI i IZSI oraz opracowanie, wdrożenie i audyt dokumentacji SZBI na zgodność z KRI/uoKSC.

1. Przeprowadzenie ankiet dojrzałości na końcu realizacji projektu w terminie określonym w regulaminie projektu w Urzędzie Gminy Krotoszyce

2. Opracowania i wdrożenia dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z zakresem stanowiącym wymaganiem w Regulaminie grantu oraz obowiązujących przepisach prawa w tym w szczególności zgodnych z Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych („KRI”); Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa w zakresie w jakim dotyczy podmiotów publicznych nie świadczących usług kluczowych („UoKSC”) 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; Ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2005 nr 64 poz. 565); Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000); Przepisami dziedzinowymi prawa UE i/lub krajowego określającego dla Zamawiającego wymagania w zakresie bezpieczeństwa informacji.

1) Opracowany i wdrożony System Zarządzania Bezpieczeństwem Informacji powinien uwzględniać wymagania Polskiej aktualnej wersji Normy PN ISO/IEC 27001:2017 oraz PN-EN ISO 22301-2019. Opracowanie/aktualizacja SZBI nie dotyczy informacji niejawnych w rozumieniu przepisów ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2018 r. poz. 412, z późn. zm.). w Urzędzie Gminy Krotoszyce,

2) Etapy wdrożenia SZBI obejmą w szczególności:

- a) Audyt obecnie funkcjonującej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.
- b) Opracowanie rekomendacji zabezpieczeń.
- c) Opracowanie i wdrożenie polityk, procedur, instrukcji SZBI.
- d) Opracowanie planów ciągłości działania, planów awaryjnych.
- e) Integracja (zapewnienie zgodności SZBI) z funkcjonującym w Urzędzie Systemem Kontroli Zarządczej.
- f) Opracowanie projektu zarządzenia w sprawie wdrożenia SZBI.
- g) Szkolenie dla kadry zarządzającej w zakresie wdrożenia SZBI.
- h) Szkolenie dla pracowników Urzędu w zakresie wdrożenia SZBI.

Etap 1. Analiza

W ramach etapu Wykonawca przeprowadzi następujące czynności

- 1) Audyt obecnie funkcjonującego Systemu Zarządzania Bezpieczeństwem Informacji w tym kontekście Zamawiającego w szczególności:
 - a) struktura organizacyjna;
 - b) role i kompetencje osób odpowiedzialnych za zarządzanie bezpieczeństwem informacji
 - c) obieg informacji w ramach SZBI
 - d) systemy informatyczne własne, powierzone w drodze umowy, porozumień, przepisu prawa;
 - e) wymagania stron zainteresowanych m.in.
 - dostawcy sprzętu, usług i oprogramowania dla Zamawiającego (Zamawiający wymaga aby Wykonawca dokona audytu wymagań w zakresie bezpieczeństwa informacji u każdego z dostawców sprzętu, usług i oprogramowania w szczególności dla obszarów prezentacji, przetwarzania, składowania informacji)
 - systemów i usług informatycznych udostępnionych oraz planowanych do udostępnienia w ramach SPR
 - klientów Zamawiającego
 - pracowników w szczególności w zakresie pracy zdalnej
 - f) zweryfikuje i zaktualizuje wykaz systemów informatycznych wykorzystywanych przez Zamawiającego wraz z wyszczególnieniem rodzaju informacji oraz kategorii osób, zależności/powiązań między systemami, poziomu ich krytyczności (ważności)
 - g) zweryfikuje obecnie stosowane zabezpieczenia fizyczne oraz techniczne stosowane przez Zamawiającego
 - h) wyspecyfikuje ryzyka jakie zostały zidentyfikowane podczas realizacji etapu „Analiza”
- 2) Sporządzi sprawozdanie z wykonania audytu obecnie funkcjonującego SZBI, w którym m.in. wyspecyfikuje; zakres rekomendowanych zmian w zakresie istniejącej SZBI w tym zalecanych/rekomendowanych zabezpieczeń fizycznych, organizacyjnych i technicznych. Wykonawca prześle sprawozdanie w formie pliku pdf
- 3) Przedstawi koncepcję aktualizacji i wdrożenia SZBI.

Etap 2. Opracowanie/aktualizacja SZBI

- 1) Na podstawie uzgodnień poczynionych pomiędzy Zamawiającym a Wykonawcą w związku z przekazaniem sprawozdania z wykonania audytu obecnie funkcjonującego SZBI, Wykonawca opracuje projekt SZBI dostosowany do uzgodnionych i przyjętych wymagań Zamawiającego.
- 2) Opracowany projekt SZBI nie jest dokumentem wiążącym dla Zamawiającego, może on podlegać modyfikacjom na skutek wzajemnych uzgodnień. Zamawiający zastrzega sobie prawo do wnoszenia uwag na każdym etapie realizacji przedmiotu zamówienia.

Etap 3. Wdrożenie i szkolenia dla kadry kierowniczej

- 1) Wykonawca opracuje materiały szkoleniowe w związku z wdrożeniem zaktualizowanego SZBI.
- 2) Wykonawca przeprowadzi szkolenia trwające m.in. 2 godziny każde dla: Kadry kierowniczej Zamawiającego, których zakres SZBI w jakimkolwiek stopniu dotyczy.
- 3) Szkolenia zostaną przeprowadzone w formie stacjonarnej lub online w siedzibie Zamawiającego w terminach uzgodnionych z Wykonawcą.

Etap 4. Wsparcie w eksploatacji SZBI

- 1) Wykonawca zapewni wsparcie w eksploatacji SZBI w okresie 2 lat od chwili wdrożenia rozwiązań

3. Przeprowadzenie w siedzibie Zamawiającego tj. w Urzędzie Gminy Krotoszyce audytu systemu bezpieczeństwa informacji wdrożonego u Zamawiającego zgodnie z §3 pkt 3 Regulaminu Konkursu Grantowego pn. "Cyberbezpieczny Samorząd" obejmujący w szczególności:

- 1) zgodnie z zapisami w § 20 ust. 2 pkt 14 rozporządzenia w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2017 poz. 2247), zwanego dalej „rozporządzeniem KRI”, zgodnie z poniższymi warunkami:
 - a) zakres audytu systemu bezpieczeństwa informacji wdrożonego w urzędzie JST obejmie zgodność z kryteriami zawartymi w § 20 ust. 2 ww. rozporządzenia KRI lub zgodność z wymaganiami normy PN-ISO/IEC 27001 oraz regulaminem grantu;
 - b) raport z audytu zostanie podpisany przez audytora dokonującego audyt systemu bezpieczeństwa informacji wdrożonego w urzędzie JST, jednostkach organizacyjnych i dostarczony w formie pliku PDF lub papierowej zgodnie z wymaganiami regulaminu grantu;;
 - c) audyt systemu bezpieczeństwa informacji wdrożonego zostanie przeprowadzony przez; audytora zewnętrznego posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz. 1999) lub; audytora wewnętrznego posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz. 1999) lub będącego audytorem zewnętrznym systemu zarządzania bezpieczeństwem informacji według normy PN-ISO/IEC 27001.
- 2) Opis metodyki sprawdzenia;
 - a) wywiad osobowy jako główna metoda analizy stanu faktycznego systemu ochrony danych osobowych,
 - b) wizja lokalna, jako ocena stanu deklarowanego ze stanem faktycznym oraz weryfikacji zabezpieczeń fizycznych i organizacyjnych newralgicznych pomieszczeń i obszarów w sprawdzanych lokalizacjach,

- c) analiza systemów informatycznych, badanie fizycznych zabezpieczeń stosowanych na stacjach roboczych losowo wybranych użytkowników lub serwerowni,
- d) analiza dokumentów, analiza przekazanych lub udostępnionych dokumentów, w celu ustalenia niezbędnego zakresu aktualizowania dokumentacji ochrony danych osobowych i bezpieczeństwa informacji,
- e) analiza witryn internetowych, analiza stron internetowych jako element badawczy mający na celu określenie spełnienia wymogów prawa w zakresie przetwarzania danych osobowych i bezpieczeństwa informacji w trakcie świadczenia usług drogą elektroniczną,
- f) testy wybranych obszarów informatycznych za pomocą dedykowanych narzędzi informatycznych i programowych.

II. Podstawowe szkolenia budujące świadomość cyberzagrożeń i sposobów ochrony dla pracowników, a także kadry oraz szkolenia specjalistyczne dla informatyków w zakresie planowanych do zastosowania środków bezpieczeństwa w ramach projektu grantowego.

1. Przeprowadzenie Szkoleń pracowników z zakresu cyberbezpieczeństwa w formie stacjonarnej lub online w Urzędzie Gminy Krotoszyce

2. Przedmiot zamówienia obejmuje szkolenie dla pracowników w zakresie określonym w regulaminie projektu. Zakres merytoryczny szkolenia: główny cel szkolenia nabycie wiedzy i umiejętności pracowników z zakresu Cyberbezpieczeństwa, bezpieczeństwa informacji i ochrony danych osobowych. Forma szkolenia – w siedzibie w czasie rzeczywistym z dodatkowym zapisem cyfrowym szkolenia umożliwiającym jego późniejsze odtworzenie. Wykonawca przekaże Zamawiającemu kopię elektroniczną zarejestrowanego szkolenia

a) Materiały szkoleniowe dla uczestników, w formie PDF lub prezentacji PowerPoint.

b) Zaświadczenia ukończenia szkolenia.

- zostaną przygotowane zgodnie z wytycznymi Zamawiającego na podstawie przesłanych list uczestników biorących udział w szkoleniu;
- będą zawierały imię i nazwisko uczestnika, tytuł wskazujący na realizowany program szkolenia, informację o terminie jego przeprowadzenia oraz liczbę godzin szkoleniowych;

c) Wsparcie poszkoleniowe uczestnikom przez dodatkowy kontakt telefoniczny z trenerem po szkoleniu

d) Opis szkolenia. Zaznajomienie uczestników z zagrożeniami, technikami ataków cyberprzestępczych oraz metodami socjotechnicznymi, ukierunkowanymi na osoby pracujące na co dzień przed komputerem, a także w jaki sposób zabezpieczać się przed takimi atakami i groźbą utraty danych. Podczas szkolenia przedstawione zostaną ryzyka wykorzystywania komputera służbowego do celów prywatnych. Szkolenie będzie dostosowane do każdego pracownika bez względu na jego wiedzę i umiejętności informatyczne. Szkolenie umożliwi zdobycie wiedzy obejmującej bezpieczne zarządzanie miejscem pracy oraz danymi.

III. Asysta i wsparcie dla realizowanych celów i zadań.

1. Asysta i wsparcie dla realizowanych celów i zadań przez okres 2 lat w zakresie dla zadań określonych w pkt. I-II oraz dodatkowe nieodpłatne wsparcie i konsultacje przez okres kolejnych 3 lat.

IV. Wymagania wobec Wykonawcy.

1. Przedmiot zamówienia zostanie wykonany przez zespół audytowy, w którym co najmniej jeden z audytorów dysponuje uprawnieniami Audytora Systemu Zarządzania Bezpieczeństwem Informacji normy PN-EN ISO/IEC 27001– wydanymi przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338) zgodnie z obowiązującymi w tym zakresie przepisami prawa oraz przy uwzględnieniu obowiązujących wytycznych. Audytorzy normy ISO 27001 lub ISO 22301 spełniający wymagania uprawnień wykazanych w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu oraz spełniający wymogi art. 15. ust. 2 pkt 2) ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Audytorzy posiadający minimum 2 letnie doświadczenie w opracowywaniu dokumentacji SZBI oraz audytowaniu systemów informatycznych w tym zagadnień cyberbezpieczeństwa w jednostkach samorządowych. Posiadają znajomość normy „chmurowych” ISO 27017, ISO 27018, Narodowych Standardów Cyberbezpieczeństwa Chmur Obliczeniowych,

2. Wykonawca powinien posiadać minimum 3 letnie doświadczenie w JST i jednostkach organizacyjnych JST w zakresie pełnienia funkcji Inspektora Ochrony Danych, Koordynatorzy ds. Cyberbezpieczeństwa.

3. Wykonawca powinien posiadać doświadczenie w opracowaniu i wdrażaniu SZBI lub podobnych wewnętrznych polityk i procedur bezpieczeństwa informacji opartych o normę ISO 27001.

4. Wykonawca powinien posiadać co najmniej 1 osobę przewidzianą do realizacji zadania posiadającą uprawnienia audytora wewnętrznego z udokumentowaną praktyką.

5. Wykonawca powinien posiadać co najmniej 1 osobę przewidzianą do realizacji zadania posiadającą co najmniej 2 letnią praktykę w jednym z następujących obszarach funkcjonowania jednostki samorządu terytorialnego:

- a) audyt wewnętrzny
- b) kontrola wewnętrzna
- c) kontrola zarządcza

6. Oświadczenie o braku powiązań osobowych lub kapitałowych z zamawiającym.