Opis Przedmiotu Zamówienia

Audyt Cyberbepieczeństwa

I. Informacje ogólne

Przedmiotem zamówienia jest usługa polegająca na przeprowadzeniu diagnozy cyberbezpieczeństwa u Zamawiającego zgodnie z wymogami Programu Operacyjnego Polska Cyfrowa na lata 2014 –2020 Działanie 5.1 Rozwój cyfrowy JST, pod kątem rozporządzenia w sprawie Krajowych Ram Interoperacyjności (KRI) oraz w oparciu o normę PN-ISO/IEC 27001 standaryzującą systemy zarządzania bezpieczeństwem informacji.

Diagnoza musi zostać przeprowadzona przez osobę posiadającą uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.

W ramach Zadania Wykonawca przeprowadzi audyt (diagnostyczny) funkcjonującego u Zamawiającego Systemu Zarządzania Bezpieczeństwem Informacji pod względem zgodności z następującymi aktami prawnymi oraz normami:

1. ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2021 r. poz. 2070, z późn. zm.) (w zakresie dotyczącym bezpieczeństwa informacji),
2. rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247) (w zakresie dotyczącym bezpieczeństwa informacji),
3. rozporządzenie 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),
4. ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560),
5. aktualne normy PN-ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO/IEC 27005, PN-ISO/IEC 27701, PN-ISO/IEC 27017 oraz PN-ISO/IEC 22301.

Podstawę audytu będą stanowiły, co najmniej:

1. wywiady z przedstawicielami Zamawiającego
2. obserwacje lub wywiady audytora, dotyczące bezpieczeństwa fizycznego i środowiskowego,
3. obserwacje lub wywiady audytora, dotyczące bezpieczeństwa serwerowni,
4. obserwacje lub wywiady audytora dotyczące bezpieczeństwa kluczowych systemów teleinformatycznych,
5. zgromadzone materiały audytowe w postaci dokumentacji bezpieczeństwa informacji i organizacyjnej obowiązującej u Zamawiającego.

Usługa ma być przeprowadzona w siedzibie Zmawiającego (Zamawiający informuje, iż dopuści wykonywanie prac w sposób zdalny w zakresie, w jakim osobista obecność Wykonawcy nie jest konieczna oraz umożliwi Wykonawcy dostęp do użytkowników i infrastruktury technicznej za pośrednictwem łącz komunikacji zdalnej)

Efektem realizacji Zadania I będzie raport z przeprowadzonego audytu bezpieczeństwa, przygotowany i przekazany Zamawiającemu w formie elektronicznej. Raport będzie zawierał co najmniej:

1. opis wykonania planu audytu,
2. opis wykorzystanych standardów,
3. ocenę spełnienia wymagań.

II. Szczegółowy Zakres Audytu

W ramach zamówienia, Wykonawca przeprowadzi diagnozę na podstawie następujących obszarów i dokumentów:

Identyfikacja systemu informacyjnego wspierającego zadanie publiczne;

- Dokumentacja dot. zarządzania incydentem,
- Dokumentacja dot. wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa,
- Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji,
- Regulacje wewnętrzne dot. zmieniającego się otoczenia,
- Inwentaryzacja sprzętu i oprogramowania,
- Analiza ryzyka utraty integralności, dostępności lub poufności informacji, postępowanie ryzykiem,
- Dokumentacja dot. zarządzania uprawnieniami,
- Dokumentacja dot. szkoleń i uświadamiania,
- Dokumentacja dot. monitorowania dostępu do informacji, nieautoryzowanych zmian i zabezpieczenia nieautoryzowanego dostępu,
- Zasady bezpiecznej pracy mobilnej,
- Dokumentacja dot. zabezpieczenia informacji przed nieuprawnionym ujawnieniem, modyfikacją, usunięciem lub zniszczeniem,
- Umowy serwisowe,
- Zasady postępowania z informacjami w celu minimalizacji ryzyka kradzieży,
- Dokumentacja dot. zapewnienia odpowiedniego poziomu bezpieczeństwa (w tym oprogramowania, utraty w wyniku awarii, ochrony przed błędami, mechanizmów kryptograficznych, bezpieczeństwa plików, zarządzania podatnościami, kontroli zgodności z regulacjami),
- Dokumentacja dot. audytu bezpieczeństwa informacji,

System informacyjny wspierający zadanie publiczne;

- Raport z audytu systemu informacyjnego,
- Dokumentacja architektury zastosowanych zabezpieczeń,
- Dokumentacja architektury sieci,
- Baza danych konfiguracji urządzeń aktywnych,
- Dokumentacja zmian w systemach informacyjnych,
- Dokumentacja dot. monitorowania w trybie ciągłym,

- Umowy z dostawcami wsparcia technicznego,
- Umowy z dostawcami usług z zakresu bezpieczeństwa teleinformatycznego,
- Raport z audytu dostawcy usług teleinformatycznych,
- Dokumentacja zabezpieczeń fizycznych i środowiskowych,
- Rejestr dostępu do dokumentacji systemu informacyjnego,

Aspekty techniczne;

- Raport z audytu serwisu WWW,
- Raport z audytu serwisu pocztowego,
- Raport z audytu lokalnych sieci teleinformatycznych,,
- Raport z audytu połączenia z siecią Internet

Aspekty organizacyjne;

- Raport z audytu organizacji zarządzania bezpieczeństwem teleinformatycznym,
- Raport z audytu procesu planowania,

III. Termin realizacji zamówienia:

Przedmiot Umowy Wykonawca zrealizuje w terminie **45 dni** od daty zawarcia Umowy z zastrzeżeniem,

1) Przeprowadzenie audytu diagnostycznego jako element rozpoznania spełniania przez funkcjonujący SZBI Zamawiającego wymagań organizacyjnych, prawnych oraz zgodności z normami ISO zakończy się do **30 dni** od daty zawarcia umowy.
2) opracowania z raportu z oceną cyberbezpieczeństwa Zamawiającego zakończy się do **15 dni** od dnia przeprowadzenia audytu.