Załącznik nr 3

Opis przedmiotu zamówienia

Usługa opracowania i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w trzech jednostkach podległych wojewodzie wielkopolskiemu

1. Przedmiot zamówienia

Przedmiotem zamówienia jest opracowanie i wdrożenie pełnej dokumentacji z zakresu Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w trzech jednostkach podległych wojewodzie wielkopolskiemu:

1. Kuratorium Oświaty w Poznaniu, ul. Kościuszki 93, 61-716 Poznań.
2. Państwowej Straży Rybackiej w Poznaniu, al. Niepodległości 16/18, 61-713 Poznań.
3. Wojewódzkim Inspektoracie Nadzoru Budowlanego w Poznaniu, al. Niepodległości 16/18, 61-713 Poznań.

Wszystkie zadania będące przedmiotem zamówienia będą realizowane oddzielnie dla każdej wskazanej jednostki.

2. Zakres przedmiotu zamówienia.

W ramach realizacji przedmiotu zamówienia Wykonawca będzie świadczył usługi doradcze i analityczne oraz opracuje i wdroży pełną dokumentację Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

Dokumentacja będąca przedmiotem zamówienia winna zapewnić zgodność z wymaganiami normy ISO/IEC 27001:2022, przepisami (KRI, RODO, KSC, NIS2) oraz uwzględniać dobre praktyki w zakresie bezpieczeństwa informacji.

Realizacja przedmiotu zamówienia realizowana będzie w niżej wymienionych etapach:

Etap I

W ramach etapu I Wykonawca:

1. Przeprowadzi analizę mającą na celu identyfikację kontekstu SZBI w poszczególnych jednostkach, na którą składa się:
   1) zapoznanie się z podstawami/wymaganiami prawnymi funkcjonowania jednostek,

2) zapoznanie się z aktualną strukturą organizacyjną i specyfiką pracy jednostek oraz poszczególnych komórek organizacyjnych,
3) inwentaryzacja zasobów informacyjnych (identyfikacja przetwarzanych informacji, środki służące do gromadzenia i przetwarzania informacji),
4) dokonanie przeglądu aktualnej dokumentacji z zakresu bezpieczeństwa informacji (polityk, procedur, instrukcji, regulaminów, wytycznych) i innych regulacji wewnętrznych oraz ich ocena pod kątem przydatności dla SZBI,
5) wykonanie innych czynności niezbędnych do prawidłowej realizacji zamówienia.

W celu przeprowadzenia ww. czynności poszczególne jednostki udostępnią niezbędne posiadane dokumenty oraz umożliwią Wykonawcy przeprowadzenie wywiadów z pracownikami w celu uzyskania informacji niezbędnych do prawidłowego wykonania przedmiotu zamówienia.

2. Sporządzenie i przekazanie sprawozdań (dla każdej jednostki oddzielnie) z przeprowadzonej analizy, o której mowa w pkt 1.
   Sprawozdanie powinno obejmować co najmniej:
   1) podsumowanie wyników przeprowadzonych czynności dla poszczególnych jednostek,
   2) propozycję rozwiązań i zmian w zakresie bezpieczeństwa informacji dla poszczególnych jednostek,
   3) przedstawienie wstępnej koncepcji SZBI adekwatnego dla poszczególnych jednostek, wynikającej z przeprowadzonej analizy ryzyka, w szczególności wskazującą na główne obszary i rodzaje procedur, które powinny być uregulowane w SZBI.

   Wykonawca przedłoży sprawozdania w formie elektronicznej w wersji edytowalnej (.docx) oraz pliku .pdf, podpisane kwalifikowanym podpisem elektronicznym lub podpisem zaufanym przez Wykonawcę.

ETAP II

W ramach etapu II Wykonawca:

1. Dokona identyfikacji aktywów, zagrożeń, podatności, skutków oraz właścicieli ryzyka.
2. Przeprowadzi analizę i ocenę ryzyka.
3. Opracuje i przygotuje do zatwierdzenia plan postępowania z ryzykiem
4. Wykona inne czynności niezbędne do prawidłowej realizacji zamówienia.

ETAP III

W ramach etapu III Wykonawca:

1. Opracuje dokumentację SZBI, na podstawie uprzednio zaakceptowanej przez poszczególne jednostki koncepcji, zgodnej z wymaganiami normy ISO/IEC 27001:2022, przepisami (KRI, RODO, KSC, NIS2) oraz uwzględniającej dobre praktyki w zakresie bezpieczeństwa informacji.
2. W ramach opracowania dokumentacji SZBI, Zabawiający wymaga aby Wykonawca uwzględnił co najmniej niżej wymienione zagadnienia:
   - cele i zakres SZBI,
   - kontekst wewnętrzny i zewnętrzny działania,
   - identyfikacja aktywów, klasyfikacja informacji oraz role i odpowiedzialność za zasoby informacyjne,
   - zasady bezpieczeństwa informacji,
   - ocena i zarządzanie ryzykiem,
   - bezpieczeństwo informacji w relacjach z podmiotami zewnętrznymi,
   - bezpieczeństwo zasobów ludzkich,
   - szkolenia i podnoszenie świadomości w zakresie bezpieczeństwa informacji,
   - bezpieczeństwo fizyczne i środowiskowe, w tym pomieszczeń specjalnego przeznaczenia,
   - bezpieczeństwo przetwarzania informacji przez pracowników (rozpoczęcie, zawieszenie, zakończenie pracy),
   - bezpieczeństwa przesyłania informacji,
   - stosowania urządzeń mobilnych, bezpiecznej pracy zdalnej oraz przenośnych nośników danych,
   - kontrola dostępu i zasady haseł oraz zabezpieczenia kryptograficzne,
   - ochrona przed szkodliwym oprogramowaniem,
   - tworzenie kopii zapasowych,
   - bezpieczeństwo sieci i transmisji danych,
   - zarządzanie sprzętem, serwis i konserwacja infrastruktury informatycznej,
   - instalacja oprogramowania,
   - ochrona własności intelektualnej,
   - zarządzanie systemami informatycznymi, w tym monitorowanie,
   - bezpieczeństwo w obszarze pozyskiwania, rozwoju i utrzymania systemów informacyjnych,
   - zarządzanie podatnościami technicznymi,

- zarządzanie incydentami bezpieczeństwa informacji,
- zasady kontroli i audytów z zakresu bezpieczeństwa informacji,
- ciągłości działania.

ETAP IV

W ramach etapu IV Wykonawca udzieli wsparcia przy wdrożeniu opracowanej dokumentacji SZBI.

Odbiór każdego z etapów zostanie potwierdzony przez Zamawiającego protokołem odbioru, podpisanym przez obie Strony.

Zamawiający wymaga przeniesienia przez Wykonawcę autorskich praw majątkowych do wszystkich dokumentów wytworzonych na rzecz jednostek objętych postepowaniem, tj. Kuratorium Oświaty w Poznaniu, Państwowa Straż Rybacka w Poznaniu i Wojewódzki Inspektorat Nadzoru Budowlanego w Poznaniu, w tym w szczególności dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), wraz z prawem do wyłącznego i nieograniczonego korzystania z nich oraz rozporządzania nimi na wszystkich polach eksploatacji, w szczególności modyfikacji, aktualizacji, tworzenia wersji pochodnych, utrwalania i zwielokrotniania (drukowanie, kserowanie), wprowadzanie do pamięci komputera i serwerów, udostępniania podmiotom trzecim w celach kontrolnych i audytowych.