Załącznik nr 1c do SWZ

Zakres zamówienia:
Przedmiotem zamówienia jest sporządzenie Ankiety Dojrzałości Cyberbezpieczeństwa, przeprowadzenie audytu oraz aktualizacja, opracowanie i wdrożenie kompleksowego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w ramach projektu „Cyberbezpieczny Samorząd w Mieście i Gminie Jabłonowo Pomorskie" współfinansowanego z *Funduszy Europejskich na Rozwój Cyfrowy (FERC) II Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa, Fundusz Europejski Fundusz Rozwoju Regionalnego (EFRR), Numer naboru FERC.02.02-CS.01-001/23*

Zakres zamówienia obejmuje:

ETAP I: Przeprowadzenie audytu przedwdrożeniowego, na potrzeby Konkursu Grantowego pn. „Cyberbezpieczny Samorząd" opublikowanym na stronie Centrum Projektów Polska Cyfrowa pod adresem http://www.gov.pl/cppc/cyberbezpieczny-samorzad.

Audyt zostanie przygotowany dla Jednostki:
Urząd Miasta i Gminy w Jabłonowie Pomorskim

ETAP II: Aktualizacja, opracowanie i wdrożenie kompleksowego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w Urzędzie Miasta i Gminy Jabłonowo Pomorskie.

W ramach etapu II Zamawiający oczekuje aktualizacji lub doskonalenia istniejącej dokumentacji a w przypadku jej braku opracowania kompleksowej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji zgodnej z wymaganiami normy PN-EN ISO/IEC 27001:2023

Zamawiający nie dopuszcza kopiowania treści ogólnodostępnych w formie nieprzetworzonej (dostępnych w Internecie). Dokumenty będą zawierać przywołania zamiast cytowania tekstów analizowanych i powszechnie dostępnych. Dokumentacja ma zawierać wyłącznie autorskie treści, powstałe w wyniku realizacji zamówienia oraz inne autorskie treści wykonawcy, które nie są publicznie dostępne. Będą opracowaniem kompletnym, wyczerpującym i dostosowanym do potrzeb organizacji, z punktu widzenia celu, któremu mają służyć.

ETAP III: przeprowadzenie audytu KRI (powdrożeniowego) systemu zarządzania bezpieczeństwem informacji oraz sporządzenie „Ankiety Dojrzałości Cyberbezpieczeństwa w Jednostkach Samorządu Terytorialnego", o których mowa w Regulaminie Konkursu Grantowego pn. „Cyberbezpieczny Samorząd" opublikowanym na stronie Centrum Projektów Polska Cyfrowa pod adresem http://www.gov.pl/cppc/cyberbezpieczny-samorzad, zwanego dalej Regulaminem.
Ankieta i audyty zostaną przeprowadzone dla Jednostki:
Urząd Miasta i Gminy w Jabłonowie Pomorskim

Szczegółowy opis przeprowadzenia aktualizacji, opracowania i wdrożenia kompleksowego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

Zamawiający jest świadomy, że dla prawidłowego wdrożenia i funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji na wszystkich etapach już od rozpoczęcia opracowywania niezbędne jest zaangażowanie, wsparcie i współdziałanie ze strony wszystkich pracowników organizacji. Poniżej wymienione pozycje w procesie budowania SZBI nie muszą stanowić katalogu zamkniętego i będą dostosowane do indywidualnych potrzeb organizacji oraz zgodnie z obowiązującymi przepisami prawa.

Zakres działań na rzecz realizacji zadania:

- Ocena bieżących praktyk w obszarze bezpieczeństwa informacji oraz analiza istniejącej dokumentacji z obszaru bezpieczeństwa informacji i ochrony danych osobowych, stosowanych zabezpieczeń technicznych i organizacyjnych.
- **Opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)**:
  - W oparciu o przeprowadzona wcześniej analizę dokonanie aktualizacji lub doskonalenie istniejącej dokumentacji a w przypadku braku opracowanie polityki bezpieczeństwa informacji zgodnej z wymaganiami normy ISO/IEC 27001.
  - Określenie celów i wskaźników na potrzeby monitorowania, pomiarów, analizy i oceny systemu zarządzania.
  - Opracowanie polityk tematycznych, procedur, wytycznych i dokumentacji operacyjnej (adekwatnie do potrzeb organizacji), w poszczególnych obszarach jak np.:
    - Zarządzania Tożsamością i Dostępem obejmujących w szczególności:
      - zasady przydzielania i odwoływania uprawnień dostępu do systemów i danych.
      - Procedura rejestracji użytkowników i zarządzania ich kontami.
      - Zarządzanie personelem i bezpieczeństwo zasobów ludzkich.
      - Monitorowanie i audyt działań użytkowników.
      - Zarządzania autoryzacją użytkowników w SI.
      - Zarządzanie w obszarze świadomości personelu - szkolenia i świadomość bezpieczeństwa:
        - Planowanie i realizacja szkoleń w zakresie bezpieczeństwa informacji dla pracowników.
        - Monitorowanie świadomości pracowników na temat zagrożeń i praktyk bezpieczeństwa.
    - Kontekst organizacji – identyfikacja wymagań i monitorowanie zmian.
    - Zarządzanie Zagrożeniami i Podatnościami
    - Zarządzanie Aktywami
    - Bezpieczeństwo fizyczne
    - Bezpieczeństwo SI i sieci
    - Bezpieczna konfiguracji i bezpieczeństwo aplikacji
    - Ochrona Informacji
    - Zarządzania Incydentami Bezpieczeństwa i Zdarzeniami Bezpieczeństwa:
      - Procedura zgłaszania, monitorowania i reagowania na zaistniałe incydenty bezpieczeństwa.
      - Monitorowanie i analiza zdarzeń związanych z bezpieczeństwem informacji.
      - Zarządzanie działaniami korygującymi i zapobiegawczymi - procedura identyfikacji, dokumentacji i realizacji działań korygujących w wyniku incydentów i nieprawidłowości w celu zapobiegania przyszłym incydentom.
    - Zarządzania Ryzykiem:
      - Analiza ryzyka związanego z informacjami i danymi.
      - Określenie strategii i zarządzania ryzykiem.

    - Monitorowanie i aktualizacja oceny ryzyka, postępowanie z ryzykiem.
  - Bezpieczeństwo relacji z Dostawcami:
    - Ocena i wybór dostawców z uwzględnieniem bezpieczeństwa informacji.
    - Monitorowanie dostawców pod kątem przestrzegania standardów bezpieczeństwa.
  - Zarządzanie monitorowaniem i audytem:
    - Monitorowanie systemów i sieci w celu wykrywania nieprawidłowości i potencjalnych zagrożeń.
    - Przeprowadzanie audytów bezpieczeństwa – planowanie, realizowanie, dokumentowanie.
  - Zarządzanie dokumentacją i zapisami, zarządzanie Politykami i Procedurami SZBI:
    - Tworzenie, kontrolowanie, przeglądy, aktualizacja i zarządzanie dokumentacją związaną z bezpieczeństwem informacji.
    - Przechowywanie, znakowanie i udostępnianie dokumentacji.
    - Tworzenie, aktualizacja i komunikacja polityk bezpieczeństwa informacji oraz procedur wewnętrznych.
  - Zarządzania Ciągłością Działania:
    - Planowanie i wdrażanie środków zapewniających ciągłość działania w przypadku awarii lub incydentów.
  - Przeglądy zarządzania ISMS
- Opracowanie Deklaracji stosowania zabezpieczeń wg wymagań Załącznika A normy PN-EN ISO/IEC 27001:2023
- Wdrożenie SZBI – działania związane z wdrożeniem do stosowania uzgodnionych procedur i zasad postępowania, konsultacje i instruktarz w zakresie dokumentowania działań, tworzenia zapisów SZBI, konsultacje i instruktaż dla osób pełniących kluczowe role w ramach SZBI.