Załącznik nr 1 - opis przedmiotu zamówienia - OPZ

Część 1 - Opracowanie i wdrożenie dokumentacji SZBI w oparciu o KRI/KSC i normę ISO27001 dla Urzędu Miejskiego w Skwierzynie oraz Ośrodka Pomocy Społecznej w Skwierzynie

1) Zakres Dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji:

SZBI powinien być zgodny z rozporządzeniem KRI i spełniać wymagania normy PN-ISO/IEC27001, w tym obejmować następujące obszary mające wpływ na bezpieczeństwo w organizacji Zamawiającego:

a) Polityka Bezpieczeństwa;
b) Organizacja bezpieczeństwa informacji;
c) Bezpieczeństwo zasobów ludzkich;
d) Zarządzanie aktywami;
e) Kontrola dostępu;
f) Kryptografia;
g) Bezpieczeństwo fizyczne i środowiskowe;
h) Bezpieczna eksploatacja;
i) Bezpieczna komunikacja;
j) Pozyskiwanie, rozwój i utrzymanie systemów;
k) Relacje z dostawcami;
l) Zarządzanie incydentami związanymi z bezpieczeństwem informacji;
m) Aspekty bezpieczeństwa w zarządzaniu ciągłością działania;
n) Zgodność z wymaganiami prawnymi i własnymi standardami.

2) W ramach poszczególnych elementów SZBI ujęte zostaną niezbędne procedury, które powinny zostać wdrożone w Urzędzie Miejskim w Skwierzynie oraz Ośrodku Pomocy Społecznej w Skwierzynie w szczególności poniższe obszary:

a) polityka bezpieczeństwa informacji:
- polityki dotyczące bezpieczeństwa informacji,
- przegląd polityk bezpieczeństwa informacji.'

b) organizacja bezpieczeństwa informacji:
- role i odpowiedzialność za bezpieczeństwo informacji,
- rozdzielanie obowiązków,
- bezpieczeństwo informacji w zarządzaniu projektami.

c) bezpieczeństwo zasobów ludzkich:
- warunki zatrudnienia,
- odpowiedzialność kierownicza,
- uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji.

d) zarządzanie aktywami:
- inwentaryzacja aktywów,
- akceptowalne użycie aktywów
- zwrot aktywów,
- klasyfikacja informacji,
- znakowanie informacji,
- postępowanie z aktywami,
- zarządzanie nośnikami wymiennymi,
- wycofywanie nośników.

e) przekazywanie nośników kontrola dostępu:
- polityka kontroli dostępu,
- dostęp do sieci i usług sieciowych,
- rejestrowanie i wyrejestrowywanie użytkowników,
- przydzielanie dostępu użytkownikom,
- zarządzanie prawami uprzywilejowanego dostępu,
- zarządzanie poufnymi informacjami uwierzytelniającymi użytkowników,
- przegląd praw dostępu użytkowników,
- odbieranie lub dostosowywanie praw dostępu,
- stosowanie poufnych informacji uwierzytelniających,
- ograniczanie dostępu do informacji,
- procedury bezpieczeństwa logowania,
- system zarządzania hasłami,
- użycie uprzywilejowanych programów narzędziowych.

f) kryptografia:
- polityka stosowania zabezpieczeń kryptograficznych,
- zarządzanie kluczami.

g) bezpieczeństwo fizyczne i środowiskowe:
- fizyczna granica obszaru bezpiecznego,
- ochrona przed zagrożeniami zewnętrznymi i środowiskowymi,
praca w obszarach bezpiecznych,
- dostawy,

- lokalizacja i ochrona sprzętu,
- bezpieczeństwo okablowania,
- konserwacja sprzętu,
- bezpieczne zbywanie lub przekazywanie do ponownego użycia,
- polityka czystego biurka i ekranu.

h) bezpieczna eksploatacja:
- dokumentowanie procedur eksploatacyjnych,
- zarządzanie zmianą,
- zarządzanie pojemnością,
- oddzielanie środowisk rozwojowych, testowych i produkcyjnych,
- zabezpieczenia przed szkodliwym oprogramowaniem,
- kopie zapasowe,
- rejestrowanie zdarzeń,
- ochrona informacji w dziennikach zdarzeń,
- rejestrowanie działań administratorów i operatorów,
- synchronizacja zegarów,
- instalacja oprogramowania w systemach produkcyjnych,
- zarządzanie podatnościami technicznymi,
- ograniczenia w instalowaniu oprogramowania.

i) bezpieczeństwo komunikacji:
- zabezpieczenia sieci,
- polityki i procedury przesyłania informacji,
- porozumienia dotyczące przesyłania informacji,
- wiadomości elektroniczne,
- umowy o zachowaniu poufności lub nieujawnieniu informacji.

j) pozyskiwanie, rozwój i utrzymanie systemów:
- analiza i specyfikacja wymagań związanych z bezpieczeństwem informacji,
- zabezpieczanie usług aplikacyjnych w sieciach publicznych,
- ochrona transakcji usług aplikacji,
- polityka bezpieczeństwa prac rozwojowych,
- ograniczenia dotyczące zmian w pakietach oprogramowania,
- outsourcing.

k) relacje z dostawcami:
- bezpieczeństwo informacji w relacji z dostawcami.

l) zarządzanie incydentami związanymi z bezpieczeństwem informacji:
- odpowiedzialność i procedury,
- zgłaszanie zdarzeń związanych z bezpieczeństwem informacji,
- zgłaszanie słabości związanych z bezpieczeństwem informacji,
- ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem,
- reagowanie na incydenty związane z bezpieczeństwem informacji,
- wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji,
- gromadzenie materiału dowodowego.

m) bezpieczeństwo informacji w zarządzaniu ciągłością działania:
- planowanie ciągłości bezpieczeństwa informacji,
- wdrożenie ciągłości bezpieczeństwa informacji.

n) zgodność:
- określenie stosowanych wymagań prawnych i umownych,
- ochrona zapisów,
- prywatność i ochrona danych identyfikujących osobę,
- regulacje dotyczące zabezpieczeń kryptograficznych.

Dokumentacja zostanie opracowana z uwzględnieniem przepisów:

1) Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. 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 2024 r. poz. 773),

2) ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2024 r.poz. 1077, z późn. zm.),

3) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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) (Dz. U. UE. L.2016.119.1),

4) zgodność z ISO/IEC 27001.

5) Wykonawca udziela gwarancji wynoszącej 12 miesięcy od daty podpisania protokołu odbioru, polegającej na wprowadzaniu niezbędnych zmian w dokumentacji i aktualizacji dokumentacji na podstawie stwierdzonych przez Zamawiającego niezgodności dokumentacji z bieżącym stanem w okresie gwarancji

Część 2 - Wdrożenie środków zarządzania ryzykiem w cyberbezpieczeństwie dla Urzędu Miejskiego w Skwierzynie oraz Ośrodka Pomocy Społecznej w Skwierzynie

1) Opracowanie kompleksowego procesu zarzadzania ryzykiem w cyberbezpieczeństwie.

Opracowanie kontekstu i wdrożenie między innymi: procesu wraz z metodyką identyfikacji i oceny ryzyka, określenie profilu ryzyka, przygotowania planu postępowania z ryzykiem w obszarze cyberbezpieczeństwa

- Opracowanie metodyki i przeprowadzenie oceny ryzyka
- Przygotowanie profilu ryzyka
- Przygotowanie planu postępowania
- Przygotowanie i przyjęcie mierników zabezpieczeń
- Uruchomienie procesu zarządzania ryzykiem
- Realizacja planu postępowania, wdrażanie zabezpieczeń technicznych
- Weryfikacja rezultatów planu
- Pomiar skuteczności zabezpieczeń
- Przygotowanie i przeprowadzenie pierwszego przeglądu zarządzania