Załącznik nr 1 do zapytania ofertowego

SE.042.4.2023

Specyfikacja przedmiotu zamówienia

1. **Przedmiotem zamówienia jest:**

przygotowanie i wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnie z wymaganiami Krajowych Ram Interoperacyjności (§ 20 rozporządzenia 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-Dz.U.2017.2247 t.j. z dnia 2017.12.05) oraz przygotowanie i wdrożenie Planu Ciągłości Działania.

2. **Informacje ogólne o środowisku Zamawiającego:**
   a) przetwarzanie informacji odbywa się w Gorzowie Wlkp., w jednym budynku,
   b) informacje przetwarzane są w formie papierowej oraz systemach informatycznych. Zamawiający zatrudnia 118 osób (12 komórek organizacyjnych),
   c) środowisko teleinformatyczne zawiera obecnie:
      - serwery zewnętrzne (kolokacja),
      - serwery wewnętrzne,
      - systemy/aplikacje internetowe (zasoby wykonawców zewnętrznych).

3. **Zakres zamówienia**

W ramach przygotowania i wdrożenia dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), Wykonawca przygotuje dokumentację:

- **Politykę Bezpieczeństwa Teleinformatycznego, która obejmuje:**
  - zasady korzystania z systemów informatycznych,
  - procedury zmiany uprawnień,
  - instrukcję wykonywania kopii zapasowej,
  - instrukcję odtworzenia kopii zapasowej,
  - rejestr komponentów bez wsparcia producentów,
  - protokół przekazania sprzętu do naprawy,
  - zarządzanie konfiguracją,
  - wzorce konfiguracji,

- rejestr komponentów środowiska teleinformatycznego,
- listę parametrów wydajności i pojemności systemów teleinformatycznych,
- zasady zapisów do raportów monitorowania wydajności i pojemności systemów teleinformatycznych Zamawiającego,
- zasady zapisów do raportów monitorowania usług zewnętrznych,
- instrukcję wycofania komponentów teleinformatycznych,
- zasady prowadzenia audytu wewnętrznego systemów teleinformatycznych,
- procedury monitorowania i przeglądu systemów teleinformatycznych,
- zasady wprowadzania i wyprowadzania danych do systemów teleinformatycznych,
- zasady szkolenia użytkowników systemów teleinformatycznych.

- **Politykę Bezpieczeństwa Informacji (PBI), która obejmuje:**
  - deklarację stosowania,
  - odwołania do innych aktów wewnętrznych Zamawiającego, dotyczących bezpieczeństwa przetwarzania informacji (np. Polityka przetwarzania danych osobowych w Starostwie Powiatowym w Gorzowie Wlkp., Instrukcja zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych w Starostwie Powiatowym w Gorzowie Wlkp., szczególne Wymagania Bezpieczeństwa oraz Procedury Bezpiecznej Eksploatacji dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych, itp.),
  - rejestr wymaganych definicji,
  - przypisanie odpowiedzialności i ról w zakresie utrzymywania SZBI.
  - Politykę Klasyfikacji Informacji,
  - Politykę Klasyfikacji Systemów Informatycznych,
  - opis metodyki szacowania ryzyka,
  - raport z procesu szacowania ryzyka
  - plan postępowania z ryzykiem
  - zasady zarządzania incydentami bezpieczeństwa,
  - zasady zarządzania rejestrem wyjątków od PBI.
  - monitorowanie i przegląd SZBI.

- **Zarządzania dostawcami usług informatycznych:**
  - wzory klauzul do umów z dostawcami,
  - przykładowe porozumienie o poufności,
  - zasady zwrotu informacji,
  - rejestr umów zawartych z dostawcami zewnętrznymi,
  - przegląd umowy i ocena dostawcy usługi.

- **W ramach Planu Ciągłości Działania (PCD) Wykonawca dokona:**
  - wdrożenia dla jednego procesu krytycznego zgodnie z normą ISO 22301.
  - szkolenia/warsztaty dla osób odpowiedzialnych za nadzorowanie PCD,
  - przekazania wzorcowej dokumentacji (wprowadzenie, klasyfikacja, zarządzanie incydentami i analiza ryzyka),
  - Wsparcia przy identyfikacji i klasyfikacji kluczowych procesów (BCP – Business Continuity Planning),
  - wsparcia przy analizie ryzyka / scenariuszach utraty ciągłości działania,
  - wsparcia przy zarządzaniu incydentami,
  - weryfikacji wdrożenia zarządzania incydentami, klasyfikacji procesów i analizy ryzyka,
  - szkolenia osób odpowiedzialne za nadzorowanie PCD (opracowywanie Minimalnych Akceptowalnych Konfiguracji - MAK-ów),
  - wsparcia przy adaptacji dokumentacji PCD (uzupełnienie kontaktów, uzupełnienie treści komunikatów, uzupełnienie personelu i zasobów sprzętowych),
  - wsparcia przy przygotowaniu MAK,
  - weryfikacji dokumentacji PCD i MAK,
  - wsparcia przy przygotowaniu instrukcji odtworzeniowych (odtwarzanie serwerów, urządzeń wirtualnych, instrukcja przełączenia),
  - testowania planów, weryfikacji instrukcji odtworzeniowych oraz wykona raport z testów.

4. **Szkolenia z zakresu Systemu Zarządzania Bezpieczeństwem Informacji i Polityki Bezpieczeństwa Informacji.**
   - Wykonawca zobowiązany jest do przygotowania i przeprowadzenia szkoleń z zakresu Systemu Zarządzania Bezpieczeństwem Informacji i Polityki Bezpieczeństwa Informacji dla wszystkich pracowników Starostwa, obejmujących co najmniej:
     - omówienie podstawowych zasad bezpieczeństwa informacji, wynikających z SZBI i PBI;
     - odpowiedzialność za naruszenie zasad SZBI i PBI;
     - zasady zgłaszania i reagowania na incydenty.
   - Szkolenia dla pracowników zostaną przeprowadzone w formie stacjonarnej w siedzibie zamawiającego.