

1. PRZEDMIOT ZAMÓWIENIA

Przedmiotem zamówienia jest:

opracowanie, weryfikacja oraz przygotowanie do wdrożenia systemów zarządzania bezpieczeństwem informacji i ciągłości działania w przedsiębiorstwie wodociągowym, z uwzględnieniem środowiska IT oraz OT (w szczególności SCADA, PLC, systemy telemetryczne), a także przeprowadzenie audytu zgodności z wymaganiami KRI.

Zakres obejmuje:

1. opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI),
2. opracowanie Planu Ciągłości Działania (PCD),
3. opracowanie i przygotowanie do wdrożenia Systemu Zarządzania Ciągłością Działania (BCM),
4. przeprowadzenie audytu zgodności z wymaganiami KRI.

2. WYMAGANIA OGÓLNE

Wykonawca zobowiązany jest do realizacji zamówienia zgodnie z:

- Rozporządzeniem w sprawie KRI,
- ustawą o Krajowym Systemie Cyberbezpieczeństwa,
- RODO,
- ISO/IEC 27001,
- ISO 22301.

Wymaga się:

- uwzględnienia specyfiki infrastruktury wodociągowej,
- uwzględnienia środowisk IT oraz OT,
- opracowania dokumentacji:
 - spójnej,
 - audytowalnej,
 - wynikającej z analizy ryzyka,
 - możliwej do wdrożenia operacyjnego.

3. SZCZEGÓŁOWY ZAKRES ZAMÓWIENIA

3.1. SZBI

Wykonawca opracuje dokumentację obejmującą co najmniej:

Dokumenty:

- Politykę Bezpieczeństwa Informacji,
- Procedurę zarządzania SZBI,
- Procedurę zarządzania ryzykiem,
- Deklarację stosowania (SoA).

Procedury:

- zarządzanie incydentami,
- zarządzanie dostępem i uprawnieniami,
- zarządzanie aktywami,
- zarządzanie podatnościami i aktualizacjami,
- zarządzanie kopiami zapasowymi,
- zarządzanie zmianą,
- zarządzanie dostawcami IT/OT.

Obszar OT:

- zabezpieczenia systemów SCADA/PLC,
- segmentację sieci IT/OT,
- kontrolę dostępu do systemów przemysłowych.

3.2. PCD

- analiza BIA,
- identyfikacja procesów krytycznych,
- określenie parametrów RTO i RPO,
- opracowanie scenariuszy awaryjnych (IT, OT, cyberatak, utrata danych).

3.3. BCM

- polityka ciągłości działania,
- procedury zarządzania ciągłością,
- harmonogram testów,
- mechanizmy przeglądu i aktualizacji.

3.4. AUDYT KRI

- analiza zgodności,
- ocena zabezpieczeń technicznych i organizacyjnych,
- raport końcowy wraz z rekomendacjami,
- przeprowadzenie ograniczonej, nieinwazyjnej weryfikacji podatności infrastruktury IT Zamawiającego, stanowiącej element identyfikacji ryzyk bezpieczeństwa informacji, obejmującej w szczególności:
 - analizę konfiguracji systemów,
 - przegląd aktualności oprogramowania,
 - identyfikację znanych podatności na podstawie publicznie dostępnych źródeł,
 - analizę zabezpieczeń logicznych i sieciowych,
- Audyt zgodności z wymaganiami KRI musi obejmować obecność kluczowego personelu Wykonawcy (w szczególności audytorów wiodących wskazanych w ofercie) w siedzibie Zamawiającego przez okres nie krótszy niż 2 dni robocze, adekwatny do zakresu audytu obejmującego środowisko IT oraz OT, w tym weryfikację procesów, systemów oraz zabezpieczeń technicznych i organizacyjnych.

4. WARUNKI UDZIAŁU W POSTĘPOWANIU

4.1. PERSONEL – WARUNEK KLUCZOWY

Wykonawca musi dysponować zespołem obejmującym:

Co najmniej **dwie osoby**, które:

- posiadają kwalifikacje audytora wiodącego zgodne z ISO/IEC 27001,

- posiadają certyfikaty wydane przez jednostki działające zgodnie z ISO/IEC 17024 lub równoważne,
- posiadają doświadczenie w audytach lub ocenie systemów bezpieczeństwa informacji.

W ramach powyższego zespołu:

- co najmniej jedna osoba musi posiadać kwalifikacje audytora wiodącego zgodne z ISO 22301.

Co najmniej jedna osoba musi posiadać:

- wykształcenie wyższe w zakresie bezpieczeństwa informacji lub cyberbezpieczeństwa.

4.2. WYMAGANIA ORGANIZACYJNE

Wykonawca musi wykazać zdolność do:

- realizacji zamówienia w sposób metodyczny,
- powiązania dokumentacji z analizą ryzyka,
- przeprowadzenia audytu i oceny systemów.

5. REALIZACJA I AUDYT ON-SITE

5.1. Osobisty udział kluczowego personelu

Wykonawca zobowiązany jest do zapewnienia osobistego udziału audytorów wiodących wskazanych w ofercie w realizacji zamówienia.

5.2. Audyt stacjonarny

Audyt zgodności z KRI oraz kluczowe czynności weryfikacyjne muszą być realizowane w formie stacjonarnej w siedzibie Zamawiającego.

WYMAGANIA SZCZEGÓŁOWE

- audyt musi być wykonany przez co najmniej dwóch audytorów wiodących wskazanych w ofercie o których mowa w pkt 4.1,
- musi obejmować:
 - analizę środowiska IT i OT,

- wywiady z pracownikami,
- przegląd dokumentacji,
- obserwację procesów,
- nie dopuszcza się realizacji audytu wyłącznie w formie zdalnej.

OGRANICZENIE ZMIAN PERSONELU

- zmiana personelu tylko za zgodą Zamawiającego,
- nowa osoba musi mieć kwalifikacje nie gorsze.

6. SPOSÓB REALIZACJI

- warsztaty,
- analiza środowiska,
- opracowanie dokumentacji,
- walidacja i testy.

7. ODBIÓR

- kompletność,
- zgodność,
- możliwość wdrożenia.

8. WYMAGANIA JAKOŚCIOWE

Wykonawca musi:

- dostarczyć dokumentację autorską,
- zapewnić spójność,
- powiązać dokumentację z analizą ryzyka,
- umożliwić audyt i testowanie.