

OPIS PRZEDMIOTU ZAMÓWIENIA

Audyt Systemu Zarządzania Bezpieczeństwem Informacji oraz elementów Systemu Zarządzania Ciągłością Działania wdrożonych w Zakładzie Gospodarki Wodno-Ściekowej w Słóńsku wraz z opracowaniem raportu końcowego

1. Przedmiot zamówienia

Przedmiotem zamówienia jest przeprowadzenie audytu Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz elementów Systemu Zarządzania Ciągłością Działania (SZCD) funkcjonujących w Zakładzie Gospodarki Wodno-Ściekowej w Słóńsku wraz z opracowaniem raportu końcowego.

Audyt ma na celu ocenę funkcjonujących rozwiązań organizacyjnych i technicznych w zakresie bezpieczeństwa informacji oraz ciągłości działania, a także ocenę zgodności z:

- § 20 ust. 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności,
- wymaganiami normy PN-EN ISO/IEC 27001 lub równoważnymi,
- wymaganiami Dyrektywy NIS2 w zakresie uproszczonej analizy luk (Gap Analysis).

Zakres audytu powinien być dostosowany do wielkości i charakteru działalności Zamawiającego.

2. Zakres audytu

2.1. Organizacja bezpieczeństwa informacji

Audyt obejmuje ocenę:

- organizacji systemu bezpieczeństwa informacji,
- obowiązujących procedur i zasad bezpieczeństwa,
- podziału odpowiedzialności za bezpieczeństwo informacji,
- sposobu zarządzania dokumentacją dotyczącą bezpieczeństwa.

2.2. Analiza danych i ocena ryzyka

Audyt obejmuje:

- identyfikację podstawowych kategorii przetwarzanych danych,

- ocenę sposobu ich przetwarzania i ochrony,
- identyfikację najważniejszych zagrożeń dla bezpieczeństwa informacji,
- ocenę ryzyka utraty poufności, integralności i dostępności informacji.

2.3. Zarządzanie dostępem

Audyt obejmuje ocenę:

- zasad nadawania, zmiany i odbierania uprawnień,
- stosowanych metod uwierzytelniania użytkowników,
- zasad korzystania z kont uprzywilejowanych,
- sposobu ewidencjonowania użytkowników.

2.4. Ochrona systemów teleinformatycznych

Ocena obejmuje:

- zabezpieczenie stacji roboczych,
- zabezpieczenie serwerów lub urządzeń przechowujących dane,
- zabezpieczenie sieci komputerowej,
- aktualizację systemów operacyjnych i oprogramowania,
- ochronę przed złośliwym oprogramowaniem.

2.5. Kopie zapasowe i ciągłość działania

Audyt obejmuje ocenę:

- sposobu wykonywania kopii zapasowych,
- możliwości odtworzenia danych,
- zabezpieczenia kopii zapasowych,
- procedur postępowania w przypadku awarii,
- rozwiązań zapewniających ciągłość działania najważniejszych procesów realizowanych przez Zakład.

2.6. Zarządzanie incydentami

Ocena obejmuje:

- sposób zgłaszania incydentów bezpieczeństwa,
- sposób dokumentowania incydentów,
- procedury reagowania na incydenty,
- działania podejmowane po wystąpieniu incydu.

2.7. Weryfikacja zgodności

Audyt obejmuje ocenę zgodności z:

- § 20 ust. 2 Rozporządzenia w sprawie Krajowych Ram Interoperacyjności,
- wymaganiami normy PN-EN ISO/IEC 27001 lub równoważnymi,
- wymaganiami Dyrektywy NIS2 w formie uproszczonej analizy luk (Gap Analysis).

3. Raport końcowy

W wyniku przeprowadzonego audytu Wykonawca opracuje raport końcowy zawierający co najmniej:

1. opis przeprowadzonych czynności audytowych;
2. ocenę zgodności z wymaganiami KRI lub PN-EN ISO/IEC 27001;
3. wyniki uproszczonej analizy zgodności z wymaganiami NIS2;
4. wykaz stwierdzonych niezgodności;
5. ocenę najistotniejszych ryzyk;
6. rekomendacje działań naprawczych wraz z określeniem priorytetów ich realizacji.

Raport zostanie przekazany:

- w wersji papierowej podpisanej przez audytora,
- w wersji elektronicznej w formacie PDF.

4. Sposób realizacji

Audyt zostanie przeprowadzony na podstawie:

- analizy dokumentacji,
- wywiadów z pracownikami,
- oględzin infrastruktury teleinformatycznej,
- przeglądu wybranych konfiguracji systemów i urządzeń.

Audyt ma charakter organizacyjno-techniczny i **nie obejmuje wykonywania testów penetracyjnych, skanowania podatności ani prób przełamania zabezpieczeń systemów teleinformatycznych.**

5. Wymagania wobec Wykonawcy

Audyt zostanie przeprowadzony przez osobę posiadającą co najmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz. U. z 2018 r. poz. 1999).

Wykonawca zobowiązany jest do zachowania poufności informacji uzyskanych podczas realizacji zamówienia.

6. Odbiór przedmiotu zamówienia

Za wykonanie zamówienia uznaje się:

- przeprowadzenie audytu zgodnie z zakresem określonym w niniejszym Opisie Przedmiotu Zamówienia;
- przekazanie raportu końcowego;
- omówienie wyników audytu z przedstawicielem Zamawiającego.

Podstawą odbioru będzie podpisany przez strony protokół odbioru.

7. Termin realizacji

Wykonawca zobowiązany jest do wykonania przedmiotu zamówienia w terminie do 15 grudnia 2026r.