Załącznik nr 5 do SWZ – Opis przedmiotu zamówienia (OPZ)

Numer zamówienia: TZP/009/26

OPIS PRZEDMIOTU ZAMÓWIENIA

„Audyt Systemu Zarządzania Bezpieczeństwem Informacji
oraz Systemu Zarządzania Ciągłością Działania”
w ramach Projektu grantowego „Poprawa cyberbezpieczeństwa
w Miejskich Wodociągach i Kanalizacji w Kędzierzynie-Koźlu Sp. z o.o.”

I. Wymagania ogólne

1. Przedmiotem zamówienia jest przeprowadzenie audytu systemu zarządzania bezpieczeństwem informacji oraz systemu zarządzania ciągłością działania wraz z opracowaniem i przekazaniem Zamawiającemu raportu z przeprowadzonego audytu systemu zarządzania bezpieczeństwem informacji oraz raportu z przeprowadzonego audytu systemu zarządzania ciągłością działania w ramach Projektu grantowego „Poprawa cyberbezpieczeństwa w Miejskich Wodociągach i Kanalizacji w Kędzierzynie-Koźlu Sp. z o.o.", zwanych dalej łącznie „Audytami".
2. Wykonawca przy świadczeniu usług jest zobowiązany uwzględnić i zastosować wymagania ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2026 r. poz. 20, z późn. zm.) wraz z nowelizacją z dnia 23 stycznia 2026 r., wdrażającą dyrektywę NIS2 (UE 2022/2555), akty wykonawcze wydane do niej oraz zgodność z wymaganiami normy PN-EN ISO/IEC 27001:2023 i PN-EN ISO 22301:2020-04 / ISO 22301:2019.
3. Wykonawca zrealizuje zamówienie w oparciu o dokumentację, którą Zamawiający dysponuje niezależnie od realizacji przedmiotu umowy i o wyjaśnienia udzielane przez Zamawiającego. W szczególności realizacja przedmiotu umowy przez Wykonawcę nie może być uwarunkowana wytwarzaniem lub uzupełnianiem dokumentów i opracowań przez Zamawiającego w związku z realizacją przedmiotu umowy, tj. Zamawiający nie może być zobowiązany do wypełniania ankiet, kwestionariuszy, sporządzania notatek itp., a informacje niezbędne Wykonawcy do wykonania przedmiotu umowy mogą być pozyskiwane wyłącznie w postaci materiałów źródłowych i wywiadu bezpośredniego.
4. Zamawiający wymaga, aby Audyty były realizowane w siedzibie Zamawiającego w czasie nie krótszym niż jeden dzień roboczy.
5. Audyty muszą zostać przeprowadzone przez tę samą osobę, spełniającą wymagania dotyczące kwalifikacji zawodowych określone przez Zamawiającego w warunku udziału w postępowaniu. Wykonawca zobowiązany jest zapewnić, że osoba przeprowadzająca Audyty będzie posiadała wymagane kwalifikacje przez cały okres realizacji zamówienia.
6. Osoba wykonująca Audyty nie może być zaangażowana w realizację zadania w zakresie cyberbezpieczeństwa wskazanego poniżej:
   1) „Zakup serwera" w ramach Projektu grantowego „Poprawa cyberbezpieczeństwa w Miejskich Wodociągach i Kanalizacji w Kędzierzynie-Koźlu Sp. z o.o.".
   2) „Dostawa i wdrożenie rozwiązań z zakresu cyberbezpieczeństwa oraz świadczenie usług w zakresie bezpieczeństwa informacji i ciągłości działania" w ramach Projektu grantowego „Poprawa cyberbezpieczeństwa w Miejskich Wodociągach i Kanalizacji w Kędzierzynie-Koźlu Sp. z o.o.".
   3) „Dostawa oprogramowania i serwerów NAS wraz z usługą wdrożenia oprogramowania" w ramach Projektu grantowego „Poprawa cyberbezpieczeństwa w Miejskich Wodociągach i Kanalizacji w Kędzierzynie-Koźlu Sp. z o.o.".
7. Wykonawcą Audytów nie może być podmiot, który realizuje lub będzie realizował zadanie wskazane w pkt 6 na rzecz Zamawiającego.

II. Kody CPV

72225000-8 – Usługi w zakresie oceny i analizy gwarancji jakości systemu
79212000-3 – Usługi audytu

III. Zakres Audytów:

1. Ustalenie relacji pomiędzy dokumentacją Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) i Systemu Zarządzania Ciągłością Działania (SZCD), a realizacją zadań z dziedziny bezpieczeństwa informacji w Miejskich Wodociągach i Kanalizacji w Kędzierzynie-Koźlu Sp. z o.o., a w szczególności realizacją zadań z następujących obszarów tematycznych:
   1) Kontekst organizacji
      - identyfikacja interesariuszy,
      - zakres SZBI,
      - analiza kontekstu organizacyjnego,
      - określenie zakresu SZCD z uwzględnieniem krytycznych usług zbiorowego zaopatrzenia w wodę i odprowadzania ścieków,
      - identyfikacja wymagań prawnych, regulacyjnych oraz interesariuszy w zakresie ciągłości działania.
   2) Przywództwo i odpowiedzialność
      - zaangażowanie kierownictwa,
      - polityka bezpieczeństwa informacji,
      - polityka ciągłości działania,
      - role i odpowiedzialności.
   3) Planowanie
      - zarządzanie ryzykiem (metodyka, rejestr ryzyk),
      - cele bezpieczeństwa informacji,
      - plan postępowania z ryzykiem,
      - cele ciągłości działania oraz planowanie ich osiągnięcia.
   4) Wsparcie
      - zasoby i kompetencje,
      - świadomość pracowników,
      - komunikacja,
      - nadzór nad dokumentacją.
   5) Działania operacyjne
      - zarządzanie dostępem,
      - zarządzanie aktywami,
      - kryptografia (jeśli dotyczy),
      - bezpieczeństwo fizyczne,
      - bezpieczeństwo systemów IT,
      - zarządzanie zmianą,
      - analiza Wpływu na Działalność (BIA - Business Impact Analysis): ocena procesów kluczowych, ustalenie wskaźników MTPD (Maximum Tolerable Period of Disruption), RTO (Recovery Time Objective) oraz RPO (Recovery Point Objective),
      - plany Ciągłości Działania (BCP) i Plany Awaryjne (DRP): opracowanie, aktualność oraz dostępność procedur ciągłości działania i odzyskiwania infrastruktury IT/OT,

- zarządzanie incydentami i komunikacja kryzysowa: procedury powiadamiania, eskalacji oraz komunikacji wewnętrznej i zewnętrznej w przypadku wystąpienia incydentu lub awarii,
- harmonogram i cykliczność przeprowadzania testów/ćwiczeń planów ciągłości działania (BCP/DRP),
- dokumentowanie wyników testów oraz wdrożenie wniosków i rekomendacji powdrożeniowych.

6) Ocena wyników
   - monitorowanie i pomiary,
   - audyty wewnętrzne,
   - przegląd zarządzania.
7) Doskonalenie
   - działania korygujące,
   - obsługa incydentów,
   - ciągłe doskonalenie SZBI.
8) Załącznik A ISO 27001 (kontrole bezpieczeństwa)
   - analiza wdrożenia zabezpieczeń (organizacyjnych, technicznych, fizycznych),
   - ocena adekwatności i skuteczności zabezpieczeń.

2. Ustalenie poziomu wdrożenia zaleceń audytu wstępnego wykonanego przed przystąpieniem do realizacji projektu.
3. Ustalenie stopnia realizacji zadań przewidzianych do realizacji w Ankiecie Dojrzałości Cyberbezpieczeństwa.

IV. Wykonawca przeprowadzi Audyty przy użyciu następujących metod:

- analiza dokumentacji SZBI i SZCD,
- wywiady z pracownikami i kierownictwem,
- przegląd systemów informatycznych,
- oględziny infrastruktury.

V. Produkty końcowe, rezultaty Audytów

Wykonawca dostarczy:

1. Raport z audytu SZBI zawierający:
   - ocenę zgodności z ISO 27001,
   - ocenę skuteczności SZBI,
   - wykaz niezgodności (major/minor),
   - identyfikację ryzyk,
   - rekomendacje działań naprawczych i doskonalących.
2. Raport z audytu SZCD zawierający:
   - ocenę zgodności wdrożonego SZCD z normą PN-EN ISO 22301,
   - ocenę kompletności i adekwatności Analizy Wpływu na Działalność (BIA) oraz Oceny Ryzyka,
   - ocenę skuteczności i realności planów ciągłości działania (BCP) oraz planów odzyskiwania po awarii (DRP),
   - ocenę systemu testowania i ćwiczeń planów ciągłości działania,

- wykaz niezgodności (major/minor),
- identyfikację ryzyk,
- rekomendacje działań naprawczych i doskonalących.

VI. Postanowienia końcowe:

Na podstawie przeprowadzonej analizy dokumentacji oraz Audytów, Wykonawca jest zobowiązany przedstawić pisemne raporty zawierające wszystkie wyniki, wnioski wraz z propozycją zmian w zakresie spełnienia wymagań. W raportach muszą zostać uwzględnione wszystkie wyniki cząstkowe z audytowanych obszarów. Spełnienie poszczególnych wymagań zostanie określone w trzyelementowej skali:

1) spełnione – oznacza, że wymaganie normy zostało całkowicie wdrożone,
2) częściowo spełnione – może zaistnieć, czy dany obszar został udokumentowany (opracowano stosowną procedurę lub przygotowano inne zabezpieczenie), ale wybrany mechanizm nie został skutecznie wdrożony (np. zdefiniowano strefy bezpieczeństwa, ale system kontroli dostępu nie funkcjonuje poprawnie); najczęstszym przypadkiem oznaczenia wymagania jako „częściowo spełnionego” jest nieskuteczne wdrożenie procedury (nie przestrzeganie zapisów procedury przez pracowników),
3) niespełnione – wymaganie niespełnione oznacza, że nie zostało ono w ogóle zidentyfikowane przez podmiot (podmiot nie jest świadomy danego zagrożenia) lub nie podjęto żadnych działań, aby wdrożyć odpowiednie mechanizmy zabezpieczające.