Nr. postępowania: ZO.1.09.2023

**Załącznik nr 3** *do zapytania ofertowego z dnia 25.09.2023r.*

# OPIS PRZEDMIOTU ZAMÓWIENIA

„Przeprowadzenie audytu cyberbezpieczeństwa Zakładu Wodociągów i Kanalizacji Sp. z o. o. w Myszkowie”

## I. Szczegółowy zakres przedmiotu zamówienia:

W ramach realizacji zamówienia Wykonawca jest zobowiązany do przeprowadzenia kompleksowego audytu cyberbezpieczeństwa (bezpieczeństwa informacji) w zakresie ustawowych obszarów działalności ZWiK (w tym w szczególności weryfikacji struktury organizacji oraz przepływu dokumentów elektronicznych, analizy zewnętrznej i wewnętrznej sieci komputerowej, analizy serwerów, testów dostępu do sieci wewnętrznej i zewnętrznej, analizy stacji roboczych, analizy kopii zapasowych, analizy systemów poczty elektronicznej, analizy ogólnego bezpieczeństwa danych i mechanizmów kontroli w ZWiK) oraz opracowania dokumentacji poaudytowej – raportu z wytycznymi do dalszego doskonalenia i rekomendacjami na przyszłość.
Celem audytu jest sprawdzenie stanu cyberbezpieczeństwa w ZWiK.

**Zakres audytu**

### 1. Audyt organizacyjny

1. Weryfikacja regulacji wewnętrznych Zamawiającego w obszarze zarządzania bezpieczeństwem informacji oraz procedur ich audytów i aktualizacji, w tym:
   a) zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji, nieuprawnionego dostępu, uszkodzeń lub zakłóceń i kradzieży środków przetwarzania informacji, w tym urządzeń mobilnych,
   b) zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość,
   c) zasad zgłaszania incydentów naruszenia bezpieczeństwa informacji i postępowania z tymi zgłoszeniami,
   d) zasad działania w przypadku publikacji informacji o podatności technicznych systemów teleinformatycznych lub dostrzeżenia nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
   e) zasad dostępu do systemów operacyjnych, w tym zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania,
2. Weryfikacja zakresów odpowiedzialności, nadanych uprawnień i adekwatnego przeszkolenia pracowników w zakresie bezpieczeństwa informacji oraz koordynacja prac związanych z zarządzaniem bezpieczeństwem informacji (w tym danych osobowych) i nadawaniem uprawnień do przetwarzania informacji,
3. Weryfikacja procedur zmiany uprawnień, w przypadku zmiany zadań pracowników, o których mowa powyżej,
4. Analiza dokumentacji dotyczącej bezpieczeństwa informacji (w tym ochrony danych osobowych) w zakresie zapisów w umowach wykonawczych i serwisowych zawieranych ze stronami trzecimi,
5. Weryfikacja aktualności spisu sprzętu i oprogramowania służącego do przetwarzania informacji oraz procedury jej aktualizacji,
6. Analiza ryzyka utraty integralności, dostępności lub poufności informacji oraz procedur minimalizujących to ryzyko, wraz z określeniem sposobu aktualizacji tej analizy.

**2. Audyt fizyczny i środowiskowy**

1. Weryfikacja granic obszaru bezpiecznego,
2. Weryfikacja zabezpieczeń wejścia/wyjścia,
3. Weryfikacja systemów zabezpieczeń pomieszczeń i urządzeń,
4. Weryfikacja zabezpieczenia informacji przed jej nieuprawnionym ujawnieniem, modyfikacją, usunięciem lub zniszczeniem (w tym bezpieczeństwa sieci wewnętrznej, komputerów i urządzeń mobilnych),
5. Weryfikacja zabezpieczenia informacji przed jej utratą (w tym systemów podtrzymania zasilania, chłodzenia i systemów alarmowych).

**3. Audyt teleinformatyczny**

1. Weryfikacja istniejących procedur zarządzania systemami teleinformatycznymi,
2. Przegląd zasobów informatycznych oraz stosowanych rozwiązań pod kątem utrzymania ciągłości działania,
   a) minimalizowaniu ryzyka utraty informacji w wyniku awarii (w tym weryfikacja procedur zarządzania kopiami zapasowymi),
   b) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
   c) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
   d) zapewnieniu bezpieczeństwa plików systemowych,
   e) Weryfikacja ochrony przed oprogramowaniem szkodliwym;
3. Analiza i ocena mechanizmów zarządzania aktualizacjami oprogramowania,
4. Weryfikacja zabezpieczeń stacji roboczych i nośników danych w szczególności tych, na których przetwarzane są dane osobowe,
5. Weryfikacja haseł (ich stosowanie, przyjęta polityka ich tworzenia oraz zmiany, mechanizmy ich przechowywania).

## II. PARAMETRY ZAMÓWIENIA

1. Audytowi podlega całość sprzętu informatycznego będącego w posiadaniu Zamawiającego:
   a) serwery fizyczne 2–szt.,
   b) komputery stacjonarne 30–szt.,
   c) notebooki 5–szt.,
   d) drukarki 16–szt.,
   e) projektor 1–szt.
2. Audyt obejmuje sieć lokalną bez podsieci.
3. ZWiK posiada jedno łącze do sieci Internet.
4. W ZWiK nie funkcjonuje usługa Active Directory.

## III. DIAGNOZA ZGODNŚCI CYBERBSEPIECZNSTWA MUSI UWZGLEDNIAĆ:

1. Rozporządzenie Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. z 2018 r. poz. 1999),
2. Ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbespieczeństwa.
3. Standard COBIT oraz normę PN-ISO/IEC 27001.
4. Przedstawienie raportu z przeprowadzonej analizy w formie papierowej i elektronicznej.