Załącznik nr 1b

Znak sprawy: KML – 60/2026

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

Szkolenie z zakresu cyberbezpieczeństwa – szkolenia dla kadry istotne z punktu widzenia wdrażanej Polityki Bezpieczeństwa Informacji oraz Systemu Zarządzania Bezpieczeństwem Informacji w obszarze IT/OT.ICS

1. Przedmiot zamówienia

Przedmiotem zamówienia jest usługa polegająca na przygotowaniu i przeprowadzeniu szkoleń z zakresu cyberbezpieczeństwa, skierowanych do kadry kierowniczej oraz osób odpowiedzialnych za obszary organizacyjne, techniczne i operacyjne, istotnych z punktu widzenia wdrażanej Polityki Bezpieczeństwa Informacji oraz Systemu Zarządzania Bezpieczeństwem Informacji.

Szkolenia obejmują osoby pełniące funkcje kierownicze, nadzorcze, koordynacyjne lub odpowiedzialne za realizację zadań związanych z bezpieczeństwem informacji, cyberbezpieczeństwem, ciągłością działania, nadzorem nad infrastrukturą IT oraz OT/ICS, a także nad procesami wspierającymi działalność przedsiębiorstwa wodociągowego.

Szkolenia będą realizowane w formule online w czasie rzeczywistym dla 3 grup w ciągu 3 dni. Pracownicy Zamawiającego będą uczestniczyli w szkoleniu przy komputerach w grupach lub indywidualnie.

Ilość uczestników: planowana liczna uczestników 85 – Zamawiający zastrzega sobie prawo do przesunięcia liczby uczestników (pracowników Zamawiającego) pomiędzy szkoleniami (*tj. pomiędzy szkoleniem dla kadry istotnym z punktu widzenia wdrażanej Polityki Bezpieczeństwa Informacji oraz Systemu Zarządzania a szkoleniem z Bezpieczeństwa Informacji w obszarze IT/OT.ICS*), przy założeniu, że całkowita liczba uczestników (pracowników Zamawiającego) nie przekroczy 362 osób, co nie będzie odstąpieniem od warunków umowy i powodem roszczeń ze strony Wykonawcy. Wynagrodzenie ryczałtowe należne Wykonawcy nie ulegnie zmianie.

Zamawiający dopuszcza zmianę formuły szkolenia po uprzednim przedstawieniu nowej propozycji przez Wykonawcę i argumentów przemawiających za wprowadzeniem zamiany oraz zaakceptowaniu jej przez Zamawiającego. Zmiana ta nie może mieć wpływu na inne warunki zamówienia, w szczególności na cenę i termin zakończenia.

2. Cel zamówienia

Celem zamówienia jest wdrożenie działań szkoleniowych umożliwiających:

- podniesienie świadomości kadry w zakresie odpowiedzialności za bezpieczeństwo informacji i cyberbezpieczeństwo,
- wsparcie wdrożenia Polityki Bezpieczeństwa Informacji oraz zasad Systemu Zarządzania Bezpieczeństwem Informacji,
- zwiększenie zdolności kadry do identyfikowania ryzyk, zagrożeń i słabości organizacyjnych oraz technicznych,

- zwiększenie zdolności kadry do podejmowania właściwych decyzji w sytuacjach związanych z incydentami bezpieczeństwa,

- ujednolicenie rozumienia ról, odpowiedzialności i obowiązków wynikających z wdrażanych zasad bezpieczeństwa,
- wsparcie bezpiecznego funkcjonowania środowisk IT oraz OT/ICS w działalności przedsiębiorstwa,
- wzmocnienie nadzoru nad realizacją polityk, procedur, środków organizacyjnych i technicznych,
- zwiększenie świadomości kadry w zakresie wymagań regulacyjnych wynikających z dyrektywy NIS2 oraz zmian ustawy o krajowym systemie cyberbezpieczeństwa.

3. Zakres zamówienia

Zakres zamówienia obejmuje w szczególności:

- opracowanie programu szkoleniowego dostosowanego do specyfiki działalności Zamawiającego,
- przygotowanie materiałów szkoleniowych w języku polskim,
- przeprowadzenie szkolenia w formule online,
- omówienie roli kadry kierowniczej i osób odpowiedzialnych w systemie zarządzania bezpieczeństwem informacji,
- omówienie znaczenia Polityki Bezpieczeństwa Informacji oraz zasad jej wdrażania i stosowania,
- omówienie podstawowych obowiązków kadry w zakresie nadzoru nad bezpieczeństwem informacji i cyberbezpieczeństwem,
- omówienie zagrożeń cyberbezpieczeństwa mogących wpływać na działalność przedsiębiorstwa wodociągowego,
- omówienie zagadnień związanych z organizacją bezpieczeństwa w środowiskach IT oraz OT/ICS,
- omówienie podstawowych wymagań regulacyjnych wynikających z dyrektywy NIS2 oraz zmian ustawy o krajowym systemie cyberbezpieczeństwa,
- omówienie zasad identyfikacji, eskalacji i zgłaszania incydentów bezpieczeństwa,
- omówienie znaczenia zarządzania ryzykiem, odpowiedzialności kierownictwa oraz monitorowania skuteczności wdrażanych działań,
- przeprowadzenie testu wiedzy weryfikującego poziom przyswojenia materiału,
- przekazanie materiałów szkoleniowych uczestnikom,
- sporządzenie potwierdzenia realizacji usługi szkoleniowej,
- wydanie imiennych certyfikatów ukończenia szkolenia.

4. Wymagania funkcjonalne

Usługa szkoleniowa musi zapewniać co najmniej:

- realizację szkolenia w formule online z możliwością udziału zdalnego uczestników,

- przekazanie treści szkoleniowych w sposób dostosowany do roli kadry kierowniczej i osób odpowiedzialnych za obszary organizacyjne, techniczne i operacyjne,
- omówienie zagadnień związanych z zarządzaniem bezpieczeństwem informacji i cyberbezpieczeństwem na poziomie organizacyjnym i nadzorczym,
- omówienie podstawowych obowiązków i odpowiedzialności kadry wynikających z wymagań regulacyjnych dotyczących cyberbezpieczeństwa,
- możliwość zadawania pytań przez uczestników w trakcie szkolenia,
- przekazanie materiałów szkoleniowych w formie elektronicznej,
- przeprowadzenie testu wiedzy po zakończeniu szkolenia,
- przekazanie Zamawiającemu informacji potwierdzającej realizację szkolenia.

5. Wymagania merytoryczne

Szkolenie musi obejmować co najmniej następujące zagadnienia:

- podstawowe pojęcia z zakresu bezpieczeństwa informacji, cyberbezpieczeństwa i zarządzania bezpieczeństwem informacji,
- rola i znaczenie Polityki Bezpieczeństwa Informacji w organizacji,
- podstawowe założenia i wymagania Systemu Zarządzania Bezpieczeństwem Informacji,
- role, odpowiedzialności i obowiązki kadry kierowniczej oraz osób odpowiedzialnych za obszary organizacyjne, techniczne i operacyjne,
- najczęstsze zagrożenia cyberbezpieczeństwa mogące wpływać na działalność organizacji, w tym phishing, ransomware, socjotechnika, nieuprawniony dostęp oraz zakłócenie dostępności systemów,
- znaczenie zarządzania ryzykiem w obszarze bezpieczeństwa informacji,
- zasady postępowania w przypadku incydentów bezpieczeństwa oraz znaczenie szybkiego zgłaszania i właściwej eskalacji zdarzeń,
- znaczenie nadzoru nad dostępem do informacji, systemów i zasobów,
- podstawowe zagadnienia świadomościowe dotyczące bezpieczeństwa środowisk OT/ICS,
- znaczenie ciągłości działania, odporności organizacyjnej oraz współpracy pomiędzy obszarami organizacyjnymi, technicznymi i operacyjnymi,
- podstawowe wymagania wynikające z dyrektywy NIS2, w szczególności w zakresie odpowiedzialności kierownictwa, środków organizacyjnych i technicznych, zarządzania ryzykiem oraz zgłaszania incydentów,
- omówienie kierunków zmian wynikających z nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa, w zakresie mającym znaczenie dla kadry kierowniczej i osób odpowiedzialnych za bezpieczeństwo,
- dobre praktyki kierownicze wspierające wdrażanie i utrzymanie zasad bezpieczeństwa informacji.

6. Wymagania organizacyjne

Usługa musi być realizowana z zachowaniem następujących warunków:

- szkolenie prowadzone będzie w języku polskim,
- szkolenie realizowane będzie w formule online,
- łączny wymiar szkolenia wynosi 6 godzin szkoleniowych z przynajmniej 1 przerwą,
- termin realizacji szkolenia zostanie uzgodniony z Zamawiającym,
- program szkolenia powinien uwzględniać specyfikę działalności przedsiębiorstwa wodociągowego oraz zakres odpowiedzialności uczestników,
- Wykonawca zapewni prowadzącego lub prowadzących posiadających wiedzę i doświadczenie w zakresie cyberbezpieczeństwa, bezpieczeństwa informacji oraz zagadnień organizacyjnych związanych z wdrażaniem SZBI,
- program szkolenia powinien uwzględniać aktualne lub projektowane wymagania prawne i regulacyjne dotyczące cyberbezpieczeństwa, w szczególności dyrektywę NIS2 oraz ustawę o krajowym systemie cyberbezpieczeństwa.

7. Przygotowanie i realizacja

Wykonawca zobowiązany jest do:

- przygotowania programu szkolenia,
- uzgodnienia z Zamawiającym terminu i sposobu realizacji szkolenia,
- przygotowania materiałów dydaktycznych,
- przeprowadzenia szkolenia online,
- zapewnienia możliwości interakcji z uczestnikami,
- przeprowadzenia testu wiedzy,
- przekazania materiałów po szkoleniu,
- przekazania informacji potwierdzającej realizację usługi.

8. Dokumentacja

Wykonawca dostarczy:

- program szkolenia,
- materiały szkoleniowe,
- prezentację lub inne materiały dydaktyczne wykorzystane podczas szkolenia,
- test wiedzy wraz z kluczem odpowiedzi albo równoważnym sposobem weryfikacji,
- zbiorczą informację o wynikach testu wiedzy,
- potwierdzenie przeprowadzenia szkolenia, np. raport, protokół, zestawienie uczestników lub dokument równoważny.

9. Szkolenie i test wiedzy

W ramach zamówienia Wykonawca przeprowadzi szkolenie obejmujące co najmniej:

- omówienie znaczenia Polityki Bezpieczeństwa Informacji i SZBI w działalności organizacji,
- omówienie odpowiedzialności kadry w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa,
- omówienie zagrożeń i ryzyk mających znaczenie dla działalności przedsiębiorstwa,
- omówienie podstawowych obowiązków wynikających z dyrektywy NIS2 oraz zmian ustawy o krajowym systemie cyberbezpieczeństwa,
- omówienie zasad reagowania na incydenty, ich zgłaszania i eskalacji,
- przeprowadzenie testu wiedzy w formie online.

Test wiedzy powinien:

- obejmować zagadnienia omówione podczas szkolenia,
- zawierać pytania zamknięte lub mieszane,
- umożliwiać ocenę poziomu przyswojenia materiału przez uczestników,
- stanowić element potwierdzający realizację efektu szkoleniowego.

10. Wymagania wobec wykonawcy

Wykonawca musi posiadać:

- doświadczenie w prowadzeniu szkoleń dla kadry kierowniczej lub osób odpowiedzialnych za obszary organizacyjne, techniczne lub operacyjne,
- kompetencje w zakresie cyberbezpieczeństwa, bezpieczeństwa informacji oraz dobrych praktyk organizacyjnych związanych z wdrażaniem zasad bezpieczeństwa,
- znajomość wymagań regulacyjnych z zakresu cyberbezpieczeństwa, w tym dyrektywy NIS2 oraz ustawy o krajowym systemie cyberbezpieczeństwa,
- doświadczenie w prowadzeniu szkoleń w formule online,
- doświadczenie w pracy z uczestnikami o różnym poziomie wiedzy technicznej i organizacyjnej,
- znajomość podstawowych zagadnień bezpieczeństwa środowisk IT oraz OT/ICS w zakresie świadomościowym i organizacyjnym.

11. Warunki odbioru

Odbiór nastąpi po:

- przeprowadzeniu szkolenia,
- przeprowadzeniu testu wiedzy,
- przekazaniu materiałów szkoleniowych,
- przekazaniu dokumentacji potwierdzającej realizację usługi.

12. Okres realizacji

Termin realizacji zamówienia: IV kwartał 2026r.

Termin przeprowadzenia szkolenia będzie ustalony z Wykonawcą wybranym w niniejszym postępowaniu.

13. Postanowienia końcowe

Wszystkie wymagania określone w niniejszym OPZ należy traktować jako minimalne.
Zamawiający dopuszcza dostosowanie programu szkolenia do specyfiki organizacyjnej i technicznej Zamawiającego, pod warunkiem zachowania celu szkolenia, minimalnego zakresu tematycznego oraz obowiązku przeprowadzenia testu wiedzy.