Znak postępowania: FDI.261.4.2026

ZAPYTANIE OFERTOWE

Przedmiot zamówienia:

Specjalistyczne szkolenia z zakresu cyberbezpieczeństwa dla kadry zarządzającej i informatyków, w zakresie zastosowanych i planowanych do zastosowania środków bezpieczeństwa w ramach Projektu grantowego (IT/OT/ICS)

Zamówienie realizowane w ramach projektu pn. „Poprawa poziomu Cyberbezpieczeństwa w Sanockim Przedsiębiorstwie Gospodarki Komunalnej Sp. z o.o. w Sanoku", współfinansowanego ze środków UE w ramach KPO, Inwestycja C3.1.1 – konkurs grantowy „Cyberbezpieczne Wodociągi" nr KPOD.05.10-CW.01-001/25 (kategoria kosztów U28, zakres 2.1.3 załącznika nr 4 do wniosku o dofinansowanie).

I. Zamawiający

Sanockie Przedsiębiorstwo Gospodarki Komunalnej Sp. z o.o., ul. Jana Pawła II 59, 38-500 Sanok; NIP: 687-00-05-556; REGON: 370301150; KRS: 0000118475; tel.: 13 464 78 00; e-mail: sekretariat@spgk.com.pl; bip.spgk.com.pl.

II. Tryb postępowania

1) Postępowanie o wartości nieprzekraczającej progu obligującego Zamawiającego (zamawiającego sektorowego) do stosowania ustawy Pzp, prowadzone na podstawie obowiązującego u Zamawiającego Regulaminu przeprowadzania postępowań o udzielenie podprogowych zamówień publicznych, dokumentu „Zasady kwalifikowania wydatków w Przedsięwzięciach realizowanych w ramach Inwestycji C3.1.1 KPO – Załącznik nr 1" oraz przepisów Kodeksu cywilnego.

2) Zapytanie zostaje upublicznione na stronie BIP Zamawiającego https://spgk.nowybip.pl/; postępowanie ma charakter otwarty. Zamawiający zastrzega prawo do zmiany warunków, zamknięcia postępowania bez wyboru oferty oraz jego unieważnienia na każdym etapie bez podania przyczyny (art. 70^1 § 3 KC).

3) Osoba do kontaktu: michal.hassinger@spgk.com.pl, e-mail: michal.hassinger@spgk.com.pl Pytania i odpowiedzi oraz zmiany treści zapytania publikowane będą na stronie BIP.

III. Opis przedmiotu zamówienia

Przedmiotem zamówienia jest przeprowadzenie (udzielenie licencji dostępowych lub realizacja w formule zdalnej/stacjonarnej) specjalistycznych szkoleń powiązanych ze środkami bezpieczeństwa wdrażanymi w ramach Projektu, w podziale na cztery odrębne Pozycje. Zamawiający DOPUSZCZA składanie ofert częściowych – na dowolną liczbę Pozycji; każda Pozycja będzie oceniana odrębnie. Wymagania minimalne dla Pozycji określa poniższa tabela; parametry wskazane stanowią wymagania minimalne.

Pozycja	**Przedmiot szkolenia i wymagania minimalne**	**Powiązany środek bezpieczeństwa (zakres 2.1.3)**
1	Kompleksowy program szkoleniowy z zakresu cyberobrony (blue team) zakończony praktycznym egzaminem, obejmujący co najmniej: analizę i reagowanie na phishing, threat intelligence, informatykę śledczą (Windows/Linux, analiza pamięci i dysków), pracę z platformą SIEM oraz proces reagowania na incydenty wg MITRE ATT&CK. Forma: dostęp on-demand przez min. 4 miesiące, min. 300 lekcji/materiałów, min. 20 laboratoriów praktycznych w przeglądarce, praktyczny egzamin scenariuszowy (min. 12 h) z co najmniej jedną bezpłatną poprawką, certyfikat ukończenia/certyfikacja bezterminowa. Liczba uczestników: 1 osoba.	System SIEM i proces obsługi incydentów (monitorowanie, detekcja, reagowanie) wdrażane w ramach Projektu
2	Kurs przygotowujący do egzaminu CISM (Certified Information Security Manager) lub równoważny program z zarządzania bezpieczeństwem informacji na poziomie menedżerskim, obejmujący: ład bezpieczeństwa informacji, zarządzanie ryzykiem, budowę i nadzór programu bezpieczeństwa oraz zarządzanie incydentami. Min. 3 dni (24 godziny) z trenerem (zdalnie lub stacjonarnie), materiały przygotowujące do	Zarządzanie wdrażanym Systemem Zarządzania Bezpieczeństwem Informacji oraz środkami bezpieczeństwa Projektu przez kadrę

	egzaminu. Egzamin certyfikacyjny NIE jest objęty zamówieniem. Liczba uczestników: 1 osoba.	
3	Szkolenie „Audytor wewnętrzny systemu zarządzania bezpieczeństwem informacji wg ISO/IEC 27001:2022”, min. 2 dni (16 godzin), obejmujące metodykę audytu wewnętrznego (ISO 19011), planowanie i przeprowadzanie audytów oraz dokumentowanie ustaleń, zakończone egzaminem wewnętrznym i certyfikatem audytora wewnętrznego. Liczba uczestników: 1 osoba.	Utrzymanie i doskonalenie wdrażanego SZBI (audyty wewnętrzne wymagane normą i procedurami)
4	Szkolenie z zakresu bezpieczeństwa sieci i systemów przemysłowych (ICS/OT), niezwiązane z rozwiązaniem konkretnego producenta, obejmujące co najmniej: architekturę i specyfikę środowisk sterowania (ICS/SCADA, PLC, HMI) oraz protokołów przemysłowych; segmentację i separację sieci IT/OT według uznanego modelu referencyjnego bezpieczeństwa systemów przemysłowych (np. model Purdue, IEC 62443, NERC CIP lub równoważny); zagrożenia i typowe wektory ataków na infrastrukturę przemysłową; monitorowanie ruchu i wykrywanie incydentów w środowisku przemysłowym; zasady reagowania na incydenty w środowisku OT. Minimum 2 dni (16 godzin) zajęć z trenerem (stacjonarnie lub zdalnie), obejmujących ćwiczenia praktyczne, warsztaty lub środowisko laboratoryjne. Liczba uczestników: 1 osoba.	Środki bezpieczeństwa środowiska OT wdrażane w Projekcie: urządzenia IDS/IPS (UTM/NGFW), separacja i segmentacja środowisk OT oraz ochrona stacji inżynierskich i serwerów SCADA (EDR)

Wspólne wymagania dla wszystkich Pozycji: szkolenia prowadzone w języku polskim lub angielskim (materiały mogą być w języku angielskim; dla Pozycji 1 dopuszcza się egzamin w języku angielskim); Wykonawca zapewni zaświadczenia/certyfikaty ukończenia dla uczestników; terminy realizacji będą uzgadniane z Zamawiającym, przy czym dostępy/licencje zostaną

uruchomione w terminie do 14 dni od zawarcia umowy, a szkolenia z trenerem zrealizowane nie później niż do 15.12.2026 r.

IV. Podstawy wykluczenia i warunki

1) Z postępowania wyklucza się Wykonawców, o których mowa w art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. (Dz.U. z 2025 r. poz. 514), oraz Wykonawców powiązanych z Zamawiającym osobowo lub kapitałowo (definicja powiązań jak w zapytaniach Zamawiającego publikowanych w ramach Projektu – oświadczenie w Załączniku nr 2).

2) W zakresie Pozycji 2 Wykonawca musi posiadać status akredytowanego dostawcy szkoleń przygotowujących do egzaminu CISM albo zapewnić program równoważny prowadzony przez trenera z aktywną certyfikacją CISM. W zakresie Pozycji 4 Wykonawca musi wykazać, że w okresie ostatnich 3 lat przeprowadził co najmniej dwa szkolenia z zakresu bezpieczeństwa systemów przemysłowych (ICS/OT), oraz zapewnić trenera posiadającego doświadczenie praktyczne w tym obszarze.

V. Kryteria oceny i składanie ofert

1) Kryterium oceny ofert: cena – 100%, odrębnie dla każdej Pozycji. Zamawiający wybierze dla każdej Pozycji ofertę z najniższą ceną brutto spełniającą wymagania.

2) Ofertę (Formularz – Załącznik nr 1 oraz Oświadczenie – Załącznik nr 2) należy złożyć do dnia [24.08.2026 r.], godz. 14:00, e-mailem na adres: cw@spgk.com.pl (skan podpisanych dokumentów lub podpis elektroniczny) albo pisemnie w sekretariacie Zamawiającego. Termin związania ofertą: 30 dni.

3) Z wybranym Wykonawcą (odrębnie dla Pozycji lub łącznie) zostanie zawarta umowa, której wzór stanowi Załącznik nr 4. Umowa obejmuje w szczególności obowiązki wynikające z finansowania ze środków KPO: poddanie się kontroli (CPPC, NASK-PIB i inne uprawnione podmioty), przechowywanie dokumentacji przez okres wymagany umową o powierzenie grantu oraz wystawienie faktury pozwalającej zidentyfikować poszczególne Pozycje. Klauzula informacyjna KPO (CPPC) stanowi Załącznik nr 3. Załącznikami do niniejszego zapytania są: Załącznik nr 1 – Formularz ofertowy; Załącznik nr 2 – Oświadczenie Wykonawcy; Załącznik nr 3 – Klauzula informacyjna KPO (CPPC); Załącznik nr 4 – Wzór umowy.

Załącznik nr 1 do Zapytania ofertowego

FORMULARZ OFERTOWY

Wykonawca (nazwa, adres, NIP): ……

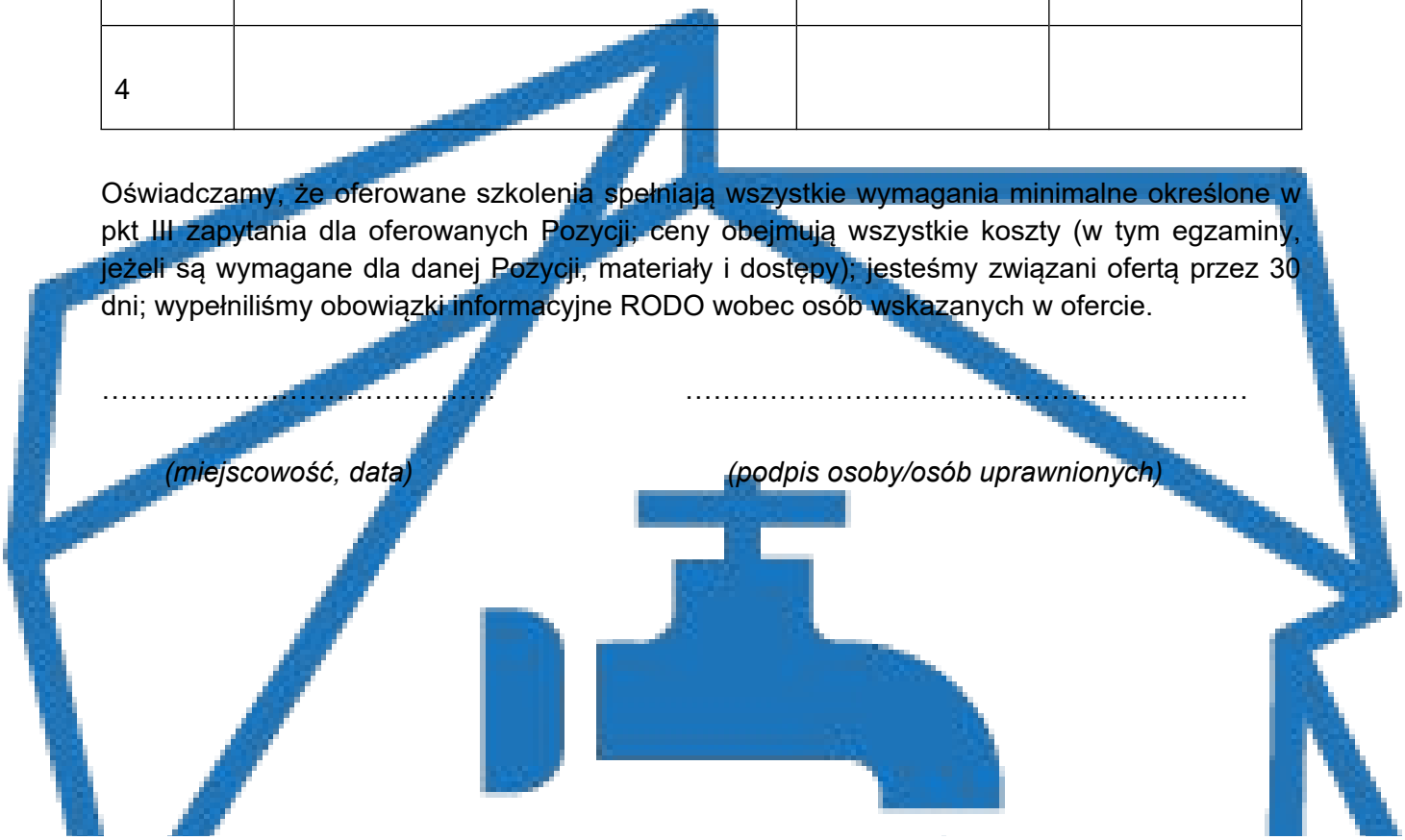
Oferujemy realizację następujących Pozycji zamówienia (wypełnić dla oferowanych Pozycji):

Pozycja	**Nazwa oferowanego szkolenia / programu (produkt, wersja)**	**Cena netto [zł]**	**Cena brutto [zł]**
1			
2			
3			
4			

Oświadczamy, że oferowane szkolenia spełniają wszystkie wymagania minimalne określone w pkt III zapytania dla oferowanych Pozycji; ceny obejmują wszystkie koszty (w tym egzaminy, jeżeli są wymagane dla danej Pozycji, materiały i dostępy); jesteśmy związani ofertą przez 30 dni; wypełniliśmy obowiązki informacyjne RODO wobec osób wskazanych w ofercie.

…… ……

(miejscowość, data) *(podpis osoby/osób uprawnionych)*



Załącznik nr 2 do Zapytania ofertowego

OŚWIADCZENIE WYKONAWCY

Oświadczam/y, że: 1) nie podlegam/y wykluczeniu na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz.U. z 2025 r. poz. 514); 2) nie jestem/eśmy powiązany/i z Zamawiającym osobowo ani kapitałowo, tj. nie zachodzą wzajemne powiązania między Zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Zamawiającego lub osobami wykonującymi w imieniu Zamawiającego czynności związane z przygotowaniem i przeprowadzeniem procedury wyboru Wykonawcy a Wykonawcą, polegające w szczególności na: uczestniczeniu w spółce jako wspólnik spółki cywilnej lub osobowej; posiadaniu co najmniej 10% udziałów lub akcji; pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika; pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia w linii bocznej lub w stosunku przysposobienia, opieki lub kurateli; 3) wszystkie informacje podane w ofercie są zgodne z prawdą.

…… ……

(miejscowość, data) *(podpis osoby/osób uprawnionych)*