ZAPYTANIE OFERTOWE

Usługi wspomagające realizację Projektu grantowego w ramach przedsięwzięcia „Cyberbezpieczne Wodociągi”

Zamawiający:

Zakład Usług Komunalnych sp. z o.o. w Łagiewnikach,
ul Słowiańska 13,
58-210 Łagiewniki

Zatwierdzam:

MACIEJ PAWEŁ WAWRZYNIAK

Elektronicznie podpisany przez MACIEJ PAWEŁ WAWRZYNIAK
Data: 2026.02.11 10:22:48 +01'00'

1. **NAZWA I ADRES ZAMAWIAJĄCEGO**
   Zakład Usług Komunalnych sp. z o.o. w Łagiewnikach, ul Słowiańska 13, 58-210 Łagiewniki
   zwany dalej „Grantobiorcą" lub „Zamawiającym".

2. **TRYB UDZIELENIA ZAMÓWIENIA**

2.1. Postępowanie ze względu na wartość szacunkową prowadzone jest w formie Zapytania ofertowego na zasadach przewidzianych w regulacjach wewnętrznych Zamawiającego.

2.2. Zamówienie jest realizowane w ramach przedsięwzięcia „Cyberbezpieczne Wodociągi" współfinansowanego przez Unię Europejską ze środków Krajowego Planu Odbudowy i Zwiększania Odporności (Inwestycja C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo).

2.3. Niniejsze zapytanie nie stanowi zobowiązania Zamawiającego do zawarcia umowy w sprawie zamówienia.

3. **OPIS PRZEDMIOTU ZAMÓWIENIA**

3.1. Przedmiotem zamówienia jest świadczenie usług, mających na celu wsparcie Grantobiorcy w realizacji Projektu grantowego w ramach przedsięwzięcia „Cyberbezpieczne Wodociągi" współfinansowanego przez Unię Europejską ze środków Krajowego Planu Odbudowy i Zwiększania Odporności w obszarze cyberbezpieczeństwa IT i OT.

3.2. W ramach realizacji przedmiotu zamówienia, Wykonawca będzie świadczyć na rzecz Zamawiającego usługi polegające w szczególności na:

a) przygotowaniu zakresu rzeczowego i merytorycznego planowanych postępowań o udzielenie zamówień publicznych niezbędnych do realizacji Projektu grantowego, zapewniających osiągnięcie wskaźników definiowanych dla Projektów grantowych realizowanych w ramach Przedsięwzięcia "Cyberbezpieczne Wodociągi" w oparciu o złożony Wniosek o przyznanie grantu;
b) współpracy przy opracowaniu dokumentacji przetargowej dla ww. zamówień publicznych w oparciu o obowiązujące przepisy i wytyczne w zakresie rzeczowym wskazanym we wniosku o przyznanie grantu;
c) udziale w charakterze biegłego w postępowaniach przetargowych z zakresu cyberbezpieczeństwa IT i OT.
d) bieżącym wsparciu merytorycznym i technicznym Zamawiającego w zakresie zgodności realizowanych działań Projektu grantowego z wymaganiami technicznymi i cyberbezpieczeństwa IT i OT
e) opiniowaniu zgodności realizacji zawartych umów z wymaganiami technicznymi i cyberbezpieczeństwa określonymi w dokumentacji projektowej
f) udziale w spotkaniach z dostawcami oprogramowanie, sprzętu i usług dostarczanych w ramach Projektu grantowego;
g) świadczeniu innych technicznych usług doradczych w zakresie nadzorowania wdrożenia zakupionych urządzeń i oprogramowania;
h) świadczeniu usług związanych ze sposobem prowadzenia dokumentacji projektowej;
i) analizie postępu prac w zakresie technicznym oraz analizie osiągnięcia wskaźników Projektu grantowego w obszarze cyberbezpieczeństwa IT i OT
j) opracowaniu sprawozdania o charakterze technicznym dotyczącego postępu rzeczowego realizacji Projektu grantowego w zakresie cyberbezpieczeństwa IT i OT.
k) realizacji usług w warunkach dostępu do informacji wrażliwych z punktu widzenia bezpieczeństwa i ciągłości działania infrastruktury wodociągowej, w tym informacji dotyczących architektury systemów IT i OT, identyfikowanych podatności, ryzyk, incydentów oraz planowanych i wdrażanych środków zabezpieczających, które wymagają podwyższonego reżimu ochrony ze względu na możliwe skutki ich nieuprawnionego ujawnienia.

3.3. Grantobiorca w celu poprawnej realizacji zamówienia wymaga, aby Wykonawca posiadał co najmniej eksperta ds. cyberbezpieczeństwa IT i OT bezpośrednio uczestniczącego w realizacji zamówienia.

3.4. Zamawiający zastrzega, że realizacja Przedmiotu zamówienia będzie możliwa wyłącznie wtedy, gdy w wyniku rozstrzygnięcia konkursu grantowego Grantobiorca zawrze Umowę o powierzenie grantu.

4. **TERMIN WYKONANIA ZAMÓWIENIA**
   Planowany okres realizacji: luty 2026 – czerwiec 2026 z możliwością przedłużenia.

5. **TERMIN ZWIĄZANIA OFERTĄ**
   Wykonawca będzie związany ofertą przez okres 30 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

6. WARUNKI UDZIAŁU W POSTĘPOWANIU

6.1. O zamówienie może ubiegać się Wykonawca, który spełnia niżej wymienione warunki dotyczące zdolności technicznej lub zawodowej.

6.2. Wykonawca spełni warunek udziału w postępowaniu, jeśli wykaże, że dysponuje lub będzie dysponował osobami zdolnymi na czas realizacji zamówienia tj.: ekspertem ds. cyberbezpieczeństwa IT i OT, który posiada:

a) co najmniej 2-letnie doświadczenie zawodowe związane z zarządzaniem w obszarze cyberbezpieczeństwa, oraz

b) posiada przynajmniej jeden ważny certyfikat lub równoważne poświadczenia (np. kwalifikację zawodową) potwierdzające możliwość wykonania zlecenia w zakresie bezpieczeństwa IT i sieci OT.

6.3. Ocena spełniania warunków udziału w postępowaniu zostanie dokonana wg formuły „spełnia – nie spełnia" w oparciu o wymagane dokumenty, wykazy i oświadczenia. Z treści załączonych dokumentów, wykazów i oświadczeń musi jednoznacznie wynikać, że Wykonawca spełnia wymagane warunki udziału w postępowaniu.

6.4. W celu potwierdzenia spełniania warunku udziału w postępowaniu składa w Formularzu ofertowym, stanowiącym załącznik nr 1 do Zapytania ofertowego, oświadczenie o spełnieniu warunków udziału.

7. OPIS KRYTERIÓW WYBORU WYKONAWCY WRAZ Z PODANIEM WAG I SPOSOBU OCENY OFERT

7.1. Wybór oferty dokonany zostanie na podstawie niżej wymienionych kryteriów:

Kryterium	znaczenie
Cena oferty brutto (C)	30%
Jakość (J)	30%
Doświadczenie (D)	40%

7.2. Za najkorzystniejszą zostanie uznana oferta, która uzyska najwyższą liczbę punktów wynikającą z sumowania punktów ze wszystkich kryteriów oceny:

$$X = C + J + D$$

7.3. Kryterium: Cena brutto (C)

Punkty zostaną przyznane według poniższego wzoru:

Liczba punktów $C = \frac{C_{ref}}{C_o} x\ 30\ pkt$, gdzie:

C_{ref} – cena referencyjna, obliczana jako mediana wszystkich ofert niepodlegających odrzuceniu,

C_o – cena brutto oferty badanej.

W przypadku liczby ofert < 3 lub braku wartości odstających, Zamawiający zastrzega możliwość zastosowania klasycznego wzoru: $C = \frac{C_{min}}{C_o}\ x\ 30\ pkt$, gdzie:

C_{min} - cena minimalna z ofert niepodlegających odrzuceniu,

C_o - cena brutto oferty badanej.

Wartości będą zaokrąglane do dwóch miejsc po przecinku.

Maksymalna liczba punktów w tym kryterium: 30 pkt.

7.4. Kryterium: Jakość (J)

W ramach kryterium jakości oceniany będzie sposób realizacji zamówienia przez osoby skierowane do jego wykonania, w zakresie jakości zapewnienia ochrony informacji wrażliwych pozyskiwanych w trakcie realizacji usług doradczych w obszarze cyberbezpieczeństwa. Kryterium odnosi się do organizacji i reżimu realizacji usługi w środowisku podwyższonego ryzyka, obejmującego w szczególności informacje dotyczące architektury systemów IT i OT, podatności, ryzyk, incydentów oraz mechanizmów zabezpieczeń infrastruktury wodociągowej a także informacji związanych z zarzadzaniem kryzysowym. Kryterium nie dotyczy cech wykonawcy jako podmiotu, lecz odnosi się wyłącznie do sposobu realizacji zamówienia przez osoby je wykonujące.

Sposób przyznawania punktów:

Opis	Punkty
Osoby realizujące Przedmiot zamówienia podlegają zewnętrznej, formalnej procedurze weryfikacji wiarygodności np. potwierdzonym posiadaniem ważnego poświadczenia bezpieczeństwa osobowego wydanego przez ABW, SKW lub inny uprawniony organ państwowy lub zagraniczny równoważny poświadczający rękojmie zachowania tajemnicy.	30 pkt
Osoby realizujące Przedmiot zamówienia realizują go w ramach udokumentowanego i certyfikowanego przez akredytowany podmiot systemu zarządzania bezpieczeństwem informacji lub równoważnych certyfikowanych zewnętrznie środków organizacyjnych i technicznych zapewniających kontrolę dostępu do informacji wrażliwych, w tym zasad need to know, rozliczalności działań oraz odpowiedzialności kontraktowej oraz posiadają zaświadczenie o niekaralności wydane nie później niż 30 dni od dnia złożenia oferty.	20 pkt.
Osoby realizujące Przedmiot zamówienia nie podlegają zewnętrznym formalnym i udokumentowanym środkom weryfikacji ani ochrony informacji wrażliwych.	0 pkt.

Punkty nie sumują się. Jeżeli osoby realizujące Przedmiot zamówienia spełniają więcej niż jedno wymaganie punktowane wg tabeli, wówczas należy podać wymaganie o najwyższej punktacji. Maksymalna liczba punktów w tym kryterium: 30 pkt.

7.5. Kryterium: Doświadczenie (D)

Punkty zostaną przyznane według poniższego wzoru: $D = D_1 + D_2$, gdzie:

D_1 - doświadczenie personelu w zarządzaniu cyberbezpieczeństwem,

D_2 - doświadczenie personelu w zarządzaniu projektami informatycznymi.

Maksymalna liczba punktów w tym kryterium: 40 pkt.

D_1 – Doświadczenie personelu w zarządzaniu cyberbezpieczeństwem

Punkty zostaną przyznane na podstawie wykazanego doświadczenia eksperta (lub osoby realizującej Przedmiot zamówienia) liczonego w pełnych latach pracy w zarządzaniu cyberbezpieczeństwem z poziomu kierowniczego, co najmniej średniego szczebla. Przez średni szczebel zarządzania należy rozumieć stanowiska m.in. CISO, pełnomocnika ds. bezpieczeństwa teleinformatycznego, dyrektora, kierownika działu/wydziału, czy menedżera projektów lub inne równoważne poziomem decyzyjności i odpowiedzialności. Jednocześnie doświadczenie oceniane będzie w kontekście zarządzania cyberbezpieczeństwem w podmiocie objętym krajowym systemem cyberbezpieczeństwa, zgodnie z poniższą tabelą.

Sposób przyznawania punktów:

Lata doświadczenia	W tym zarządzanie cyberbezpieczeństwem w podmiocie objętym KSC?	Punkty
3 lata i więcej	tak	8 pkt.
co najmniej 2 lata	tak	6 pkt.
3 lata i więcej	nie	4 pkt.
co najmniej 2 lata	nie	2 pkt.

Maksymalna liczba punktów w tym podkryterium: 8 pkt.

D_2 – Doświadczenie personelu w zarządzaniu projektami informatycznymi

Punkty zostaną przyznane na podstawie wykazanego doświadczenia eksperta (lub osoby realizującej Przedmiot zamówienia) liczonego w pełnych latach pracy lub liczby zrealizowanych projektów w charakterze osoby odpowiedzialnej za projekt lub kierującej projektem obejmującym zakresem komponent cyberbezpieczeństwa, budowę infrastruktury IT i/lub oprogramowania teleinformatycznego. Jednocześnie doświadczenie oceniane będzie w kontekście projektów współfinansowanych lub finansowanych ze środków UE, zgodnie z poniższą tabelą.

Sposób przyznawania punktów:

Lata doświadczenia lub zrealizowane projekty	W tym projekt(y) finansowany(e) ze środków UE?	Punkty
powyżej 10 lat lub co najmniej 20 projektów	tak	32 pkt.
5-9 lat lub co najmniej 10 projektów	tak	28 pkt.
2-4 lata lub co najmniej 5 projektów	tak	24 pkt.
1 rok lub co najmniej 1 projekt	tak	20 pkt.
powyżej 10 lat lub co najmniej 20 projektów	nie	16 pkt.
5-9 lat lub co najmniej 10 projektów	nie	12 pkt.
2-4 lata lub co najmniej 5 projektów	nie	8 pkt.
1 rok lub co najmniej 1 projekt	nie	4 pkt.
brak doświadczenia lub projektu	nie dotyczy	0 pkt.

Maksymalna liczba punktów w tym podkryterium: 32 pkt.

8. OPIS SPOSOBU PRZYGOTOWANIA I ZŁOŻENIA OFERTY

8.1 Oferta powinna być sporządzona w języku polskim, zgodnie ze wzorem Formularza Ofertowego.
8.2 Wykonawca określa całkowitą cenę oferty za realizację przedmiotu zamówienia poprzez wskazanie w formularzu ofertowym: ceny netto i brutto oraz kwoty podatku VAT.
8.3 Łączna cena oferty brutto musi uwzględniać wszystkie koszty związane z realizacją przedmiotu zamówienia.
8.4 Cena musi być wyrażona w złotych polskich, z dokładnością do dwóch miejsc po przecinku.
8.5 Do oferty należy załączyć:
a) Pełnomocnictwo – jeżeli dotyczy.
8.6 Wykonawca ma prawo złożyć tylko jedną ofertę, zawierającą jedną, jednoznacznie opisaną propozycję.
8.7 Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.
8.8 Dokumenty sporządzone w języku obcym należy złożyć wraz z tłumaczeniem na język polski.

9 MIEJSCE ORAZ TERMIN SKŁADANIA OFERT

9.1 Termin składania ofert: 16.02.2026 r. godz. 08:00

9.2 Ofertę należy przesłać drogą elektroniczną przed upływem terminu składania ofert na adres e-mail: zamowienia@zuk-lagiewniki.pl. W tytule wiadomości należy wpisać: **Usługi wspomagające realizację Projektu grantowego w ramach przedsięwzięcia „Cyberbezpieczne Wodociągi”**

9.3 W dniu otwarcia ofert, w godzinach od 08:00 do 08:30, Wykonawca zobowiązany jest przesłać hasło umożliwiające odszyfrowanie oferty na adres e-mail: przemyslaw.pikul@zuk-lagiewniki.pl.
W treści wiadomości należy wskazać nazwę Wykonawcy oraz numer postępowania.

9.4 Otwarcie ofert nastąpi w dniu 16.02.2026 roku o godz. 08:30 w siedzibie Zamawiającego.

9.5 Oferty złożone po terminie nie będą rozpatrywane. O zachowaniu terminu złożenia oferty decyduje data i godzina wpływu oferty.

10 INFORMACJE DODATKOWE DOTYCZĄCE ZAMÓWIENIA

10.1 Zamawiający nie dopuszcza możliwość składania ofert częściowych.

10.2 Zamawiający nie przewiduje udzielenia zamówień uzupełniających.

10.3 Zamawiający nie dopuszcza możliwości składania ofert wariantowych.

10.4 W przypadku wątpliwości co do treści złożonej oferty lub jakichkolwiek informacji składanych przez Wykonawców, Zamawiający może zastosować instytucję wezwania do wyjaśnień.

10.5 Zamawiający zastrzega sobie prawo rezygnacji z zamówienia lub anulowania postępowania na dowolnym etapie.

10.6 Zamawiający poprawi w ofercie oczywiste omyłki pisarskie.

10.7 Zamawiający odrzuca ofertę, jeżeli:

a) Wykonawca nie złoży wyjaśnień, o których mowa w ust. 10.4 we wskazanym terminie lub mimo ich złożenia oferta Wykonawcy podlega odrzuceniu,

b) jej treść nie odpowiada treści Zapytania Ofertowego.

Załączniki do Zapytania Ofertowego:

1. Załącznik nr 1 - Formularz ofertowy
2. Załącznik nr 2 - Wzór umowy
3. Załącznik nr 3 – Instrukcja szyfrowania ofert
4. Załącznik nr 4 - Rodo