Ogłoszenie

Numer

2026-123150-293946

Id

293946

Powstaje w kontekście projektu

KPOD.05.10-IW.06-0008/25 - Cyberbezpieczne Wodociągi

Tytuł

„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.”
Umowa o powierzenie grantu o numerze KPOD.05.10-CW.01-001/25/0529/KPOD.05.10--CW.01-001/25/2026

Zamówienia uzupełniające

Zamawiający nie przewiduje udzielania zamówień uzupełniających.

Warunki zmiany umowy

Zamawiający przewiduje możliwość zmian postanowień umowy. Szczegółowe zasady wprowadzania zmian określone zostały w Projektowanych postanowieniach umowy stanowiących Załącznik nr 9 do Specyfikacji Warunków Zamówienia.

Załączniki

Dodane do ogłoszenia w obowiązującej wersji z dn. 2026-10-06

1. TZP_007_26_Specyfikacja Warunków Zamówienia (SWZ) na dostawy.pdf
2. Załącznik nr 1 do SWZ - Formularz Ofertowy.docx

3. Załącznik nr 1A do SWZ - Szczegółowa specyfikacja dostaw - zapora bezpieczeństwa.docx
4. Załącznik nr 2 do SWZ - Ośw. o niepodl. wykl. oraz spełn. war. udziału w postęp. - Wyk._Wyk. ws.docx
5. Załącznik nr 2a do SWZ - Ośw. o niepodl. wykl. oraz spełn. war. udziału w postęp. - Podmiot udo.docx
6. Załącznik nr 3 do SWZ - Wzór zobow. podm. do oddania do dysp. wyk. niezb. zasobów na potrzeby r.docx
7. Załącznik nr 4 do SWZ - Wzór wykazu usług.docx
8. Załącznik nr 5 do SWZ - Wzór wykazu dostaw.docx
9. Załącznik nr 6 do SWZ - Wzór wykazu osób.docx
10. Załącznik nr 7 do SWZ - Wzór gwarancji zabezpieczenia należytego wykonania umowy.docx
11. Załącznik nr 8 do SWZ - Opis przedmiotu zamówienia (OPZ).pdf
12. Załącznik nr 9 do SWZ - Projektowane postanowienia umowy (PPU).pdf
13. Załącznik nr 10 do SWZ - Ośw. Wyk. - SIEM-SOAR i dokumentacja.docx
14. Załącznik nr 11 do SWZ - Klauzula informacyjna KPO (CPPC jako OOW).PDF
15. Załącznik nr 12 do SWZ - Informacja o przetwrazaniu danych osobowych.docx

Czy dopuszczalna oferta częściowa?

NIE

Data opublikowania ogłoszenia

2026-10-06

Data ostatniej zmiany

2026-10-06

Termin składania ofert

2026-10-21 11:00:00

Planowany termin podpisania umowy

2026-11

Dane adresowe ogłoszeniodawcy

> Miejskie Wodociągi i Kanalizacja w Kędzierzynie-Koźlu
> Spółka z o.o.
> Filtrowa 14
> 47-200 Kędzierzyn-Koźle
> NIP: 7490005208

Osoby do kontaktu

> Jolanta Stach
> tel.: 77 480 13 07
> e-mail: j.stach@mwik.com.pl

Części zamówienia

-

Część: 1

Tytuł części 1

Dostawa i wdrożenie rozwiązań cyberbezpieczeństwa

Czy dopuszczalne oferty wariantowe

NIE

Przedmioty zamówienia do części 1

Typ

Dostawa

Podkategoria

Sprzęt IT

Opis

1. Nazwa przedmiotu zamówienia.
„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.”

2. Przedmiotem zamówienia jest podniesienie poziomu cyberbezpieczeństwa środowisk IT i OT przedsiębiorstwa wodociągowego przez realizację czterech zadań: rozwój kompetencji i systemów zarządzania wraz z usługą Security Awareness; wdrożenie SIEM/SOAR z modułem GRC; dostawa i wdrożenie IDS OT oraz jednej zapory bezpieczeństwa do separacji IT/OT; monitoring SOC.

3. Szczegółowy opis przedmiotu zamówienia określa Załącznik nr 8 do Specyfikacji Warunków Zamówienia – Opis przedmiotu zamówienia (OPZ), Załącznik nr 9 do Specyfikacji Warunków Zamówienia – Projektowane postanowienia umowy (PPU).

4. Wykonawca wraz z ofertą zobowiązany jest do przedłożenia Zamawiającemu – Załącznika nr 1A do Specyfikacji Warunków Zamówienia – Szczegółowa specyfikacja dostaw (dostawa i wdrożenie jednej zapory bezpieczeństwa).

5. Termin realizacji przedmiotu zamówienia – 18 grudnia 2026 r.

Okres gwarancji

• 60 miesięcy wsparcia producenta dla rozwiązania systemu SIEM/SOAR; • 36 miesięcy wsparcia technicznego i serwisu producenta oprogramowania oraz dostarczonych sond; •60 miesięcy gwarancji na zaporę

Kody CPV

32420000-3 Urządzenia sieciowe
48730000-4 Pakiety oprogramowania zabezpieczającego
72222000-7 Usługi w zakresie systemów informacji lub strategicznej analizy technologicznej oraz usługi w zakresie planowania
72224000-1 Usługi doradcze w zakresie zarządzania projektem
72250000-2 Usługi w zakresie konserwacji i wsparcia systemów
72253000-3 Usługi pomocy komputerowej i podobne
72260000-5 Usługi w zakresie oprogramowania
72263000-6 Usługi wdrażania oprogramowania
72268000-1 Usługi dostawy oprogramowania
79111000-5 Usługi w zakresie doradztwa prawnego
80510000-2 Usługi szkolenia specjalistycznego
80533100-0 Usługi szkolenia komputerowego

Miejsca realizacji

adres

Kraj
Polska

Województwo
opolskie

Powiat
kędzierzyńsko-kozielski

Gmina
Kędzierzyn-Koźle

Miejscowość
Kędzierzyn-Koźle

Warunki, jakie musi spełniać oferent

Typ
Wiedza i doświadczenie

Opis

1) Wykonawca spełni warunek, jeżeli wykaże, że posiada doświadczenie w postaci należytego wykonania co najmniej:
a) jednego zamówienia polegającego na opracowaniu i wdrożeniu dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), o wartości zamówienia nie mniejszej niż 30 000 zł brutto;
b) dwóch zamówień polegających na świadczeniu usług Security Operations Center (SOC), o wartości każdego zamówienia nie mniejszej niz 50 000 zł brutto, w tym co najmniej jednego zamówienia świadczonego na rzecz podmiotu z sektora wodno-kanalizacyjnego;
c) dwóch zamówień polegających na dostawie i wdrozeniu systemu przeciwdziałającemu cyberzagrozeniom typu SIEM/SOAR, o wartości każdego zamówienia nie mniejszej niż 250 000 brutto.
Zamówienia te muszą być wykonane, a w przypadku świadczeń powtarzających się lub ciągłych również wykonywane, w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie.
Dla każdego świadczenia powtarzającego się lub ciągłego, zamawiający uzna warunek za spełniony, gdy wykonawca zrealizował zakres zamówienia odpowiadający wymaganiom określonym w niniejszym warunku, w tym osiągnął wymaganą wartość tego zakresu.

Typ

Lista wymaganych dokumentów/oświadczeń

Opis

1. DOKUMENTY SKŁADANE WRAZ Z OFERTĄ.
1.1. Do oferty należy złożyć:
1) Formularz ofertowy, sporządzony zgodnie ze wzorem stanowiącym Załącznik nr 1 do Specyfikacji Warunków Zamówienia.
2) Szczegółową specyfikację dostaw (dostawa i wdrożenie jednej zapory bezpieczeństwa) – Załącznik nr 1A do Specyfikacji Warunków Zamówienia.
3) Oświadczenie o niepodleganiu wykluczeniu oraz spełnianiu warunków udziału w postępowaniu. Oświadczenie składają odrębnie:
a) wykonawca/każdy spośród wykonawców wspólnie ubiegających się o udzielenie zamówienia (wzór oświadczenia stanowi Załącznik nr 2 do Specyfikacji Warunków Zamówienia).
W takim przypadku oświadczenie potwierdza brak podstaw wykluczenia wykonawcy oraz spełnianie warunków udziału w postępowaniu w zakresie, w jakim każdy z wykonawców wykazuje spełnianie warunków udziału w postępowaniu.
b) podmiot udostępniający zasoby, na którego potencjał powołuje się wykonawca celem potwierdzenia spełniania warunków udziału w postępowaniu, jeżeli dotyczy (wzór oświadczenia stanowi Załącznik nr 2a do Specyfikacji Warunków Zamówienia).

W takim przypadku oświadczenie potwierdza brak podstaw wykluczenia podmiotu oraz spełnianie warunków udziału w postępowaniu w zakresie, w jakim podmiot udostępnia swoje zasoby wykonawcy.
4) Odpis lub informację z Krajowego Rejestru Sądowego, Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub innego właściwego rejestru potwierdzającego, że osoba działająca w imieniu wykonawcy jest umocowana do jego reprezentowania.
5) Pełnomocnictwo lub inny dokument potwierdzający umocowanie do reprezentowania wykonawcy, gdy umocowanie osoby składającej ofertę nie wynika z dokumentów opisanych w pkt 1.1.4).
6) W przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia:
a) pełnomocnictwo, z treści którego będzie wynikało umocowanie do reprezentowania ich w postępowaniu o udzielenie zamówienia albo do reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia;
b) oświadczenie, o którym mowa w pkt 7.3. Specyfikacji Warunków Zamówienia (zamawiający dopuszcza złożenie tego oświadczenia na formularzu ofertowym).
7) Zobowiązanie podmiotu udostępniającego zasoby do oddania lub inny podmiotowy środek dowodowy potwierdzający, że wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami podmiotów – wskazany w pkt 8.3. oraz 8.4. Specyfikacji Warunków Zamówienia, jeżeli dotyczy (wzór stanowi Załącznik nr 3 do Specyfikacji Warunków Zamówienia).
8) Oświadczenie, o którym mowa w pkt 11.1. Specyfikacji Warunków Zamówienia, zawierające link do udostępnionej wersji demonstracyjnej oferowanego systemu SIEM/SOAR oraz aktualnej dokumentacji technicznej i funkcjonalnej systemu – przedmiotowy środek dowodowy (wzór stanowi Załącznik nr 10 do Specyfikacji Warunków Zamówienia).
9) Dowód wniesienia wadium.
1.2. Wykonawca nie jest zobowiązany do złożenia dokumentu rejestrowego, o których mowa w pkt 1.1.4), jeżeli zamawiający może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, o ile wykonawca wskazał dane umożliwiające dostęp do tych dokumentów.
1.3. Zapisy pkt 1.1.5) stosuje się odpowiednio do osoby działającej w imieniu wykonawców wspólnie ubiegających się o udzielenie zamówienia.
1.4. Zapisy pkt 1.1.4), 1.1.5) i 1.2. stosuje się odpowiednio do osoby działającej w imieniu podmiotu udostępniającego zasoby na zasadach określonych w pkt 8.1. - 8.4. Specyfikacji Warunków Zamówienia.

2. OŚWIADCZENIA I DOKUMENTY SKŁADANE NA WEZWANIE, PODMIOTOWE ŚRODKI DOWODOWE.
2.1. Zamawiający przed wyborem najkorzystniejszej oferty wezwie wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie, nie krótszym niż 5 dni od dnia wezwania, aktualnych na dzień złożenia, następujących podmiotowych środków dowodowych:
2.1.1. Potwierdzających spełnianie warunków udziału w postępowaniu: zgodnie z pkt 13.1.1. Specyfikacji Warunków Zamówienia.
2.1.2. Potwierdzających brak podstaw wykluczenia wykonawcy z udziału w postępowaniu: nie

dotyczy.
2.1.3. Dokumenty podmiotów zagranicznych: nie dotyczy.

Typ

Dodatkowe warunki udziału

Opis

1) Wykonawca spełni warunek, jeżeli wykaże, że posiada ważną akredytację Trusted Introducer dla zespołu SOC, na poziomie co najmniej Accredited.

2) Wykonawca spełni warunek, jeżeli wykaże, że posiada aktualny certyfikat systemu zarządzania bezpieczeństwem informacji wg normy ISO/IEC 27001 lub równowazny, przy czym za równowazne Zamawiający uznaje wyłącznie ustandaryzowane systemy międzynarodowe, stosowane na terenie UE.

3) Wykonawca spełni warunek, jeżeli wykaże, że posiada aktualny certyfikat systemu zarządzania ciągłością działania wg normy PN-EN ISO 22301 lub równowazny, przy czym za równowazne Zamawiający uznaje wyłącznie ustandaryzowane systemy międzynarodowe, stosowane na terenie UE.

4) Wykonawca spełni warunek, jeżeli wykaże, że posiada aktualny certyfikat potwierdzający stosowanie zabezpieczeń usług chmurowych wg normy ISO/IEC 27017 lub równowazny, przy czym za równowazne Zamawiający uznaje wyłącznie ustandaryzowane systemy międzynarodowe, stosowane na terenie UE.

5) O udzielenie zamówienia mogą ubiegać się wykonawcy, którzy nie podlegają wykluczeniu. Podstawy wykluczenia z postępowania określono w pkt 10 Specyfikacji Warunków Zamówienia.

6) Oferta musi być zabezpieczona wadium w wysokości: 9 000,00 PLN. Wymagania dotyczące wadium określono w pkt 15 Specyfikacji Warunków Zamówienia.

Typ

Osoby zdolne do wykonania zamówienia

Opis

1) Wykonawca spełni warunek, jeżeli wykaże, że dysponuje zespołem osób zdolnych do realizacji z amówienia w zakresie Security Operation Center, które zostaną skierowane do wykonywania zamówienia, spełniających nizej wymienione wymagania:
a) co najmniej jedną osobą posiadającą łącznie certyfikat w zakresie bezpieczeństwa IT o

fensywnego - CRTP (Certified Red Team Professional) lub OSCP (Offensive Security Certified P rofessional) lub PNTP (Professional Network Penetration Tester) i certyfikat CompTIA CySa+ lub r ównowazny;
b) co najmniej 4 osobami posiadającymi certyfikat w zakresie bezpieczeństwa IT defensywnego - SC-200 (Microsoft Certified Security Operations Analyst) lub CDCP (Cyber Defense Certified P rofessional) lub OSIR (OffSec Incident Responder) lub równowazny;
c) co najmniej jedna osoba posiadająca certyfikat Microsoft AZ-500 (Microsoft Certified Azure Security Engineer) lub równowazny;
d) co najmniej jedną osobą posiadającą łącznie certyfikaty CompTia Security + lub równowazny i CompTIA CySA+ lub równowazny.

2) Wykonawca spełni warunek, jeżeli wykaże, że dysponuje co najmniej jedną osobą zdolną do realizacji zamówienia w zakresie utrzymania i wsparcia systemu SIEM SOAR oraz modelowania z agrozeń i wsparcia powdrozeniowego, posiadającą łącznie certyfikaty:
a) CISM - Certified Information Security Manager;
b) CISA - Certified Information Systems Auditor;
c) CRISC - Certified in Risk and Information Systems Control;
d) ITIL Foundation Certificate in IT Service Management;
e) SIM3 (Security Incident Management Maturity Model).

3) Wykonawca spełni warunek, jeżeli wykaże, że dysponuje osobami zdolnymi do realizacji zamówienia, skierowanymi do wykonywania zamówienia, posiadającymi niżej wymienione doświadczenie:
a) co najmniej jedna osoba posiada doświadczenie w przeprowadzeniu co najmniej jednego szkolenia dotyczącego praktycznego stosowania polityk bezpieczeństwa lub SZBI;
b) co najmniej jedna osoba posiada doświadczenie w przeprowadzeniu co najmniej jednego szkolenia dla kierownictwa oraz co najmniej jednego szkolenia technicznego z zakresu cyberbezpieczeństwa, a także doświadczenie pozwalające na omówienie zależności IT/OT; przy czym obydwa szkolenia może prowadzić ta sama osoba;
c) co najmniej jedna osoba posiada doświadczenie w co najmniej jednej autoryzowanej kampanii socjotechnicznej zakończonej działaniem edukacyjnym;
d) co najmniej jedna osoba posiada doświadczenie w przygotowaniu i przeprowadzeniu co najmniej jednego ćwiczenia z zakresu reagowania na incydenty, ciągłości działania lub zarządzania kryzysowego;
e) co najmniej jedna osoba posiada doświadczenie w opracowaniu lub wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), obejmującym zarządzanie ryzykiem, opracowanie dokumentacji oraz uruchomienie zasad SZBI, z uwzględnieniem zależności pomiędzy procesami operacyjnymi a środowiskiem IT;
f) co najmniej jedna osoba posiada doświadczenie w co najmniej jednym cyklu utrzymania lub

przeglądu SZBI, obejmującym zarządzanie ryzykiem, działania korygujące oraz wsparcie procesu decyzyjnego kierownictwa;
g) co najmniej jedna osoba posiada doświadczenie w opracowaniu Business Continuity Plan (BCP) i Disaster Recovery Plan (DRP), obejmującym określenie zależności i priorytetów odtworzenia oraz opracowanie lub aktualizację instrukcji odtworzeniowych; wymagania określone w niniejszym punkcie mogą zostać spełnione w ramach jednej usługi;
h) co najmniej jedna osoba posiada doświadczenie w ustanowieniu lub przeglądzie zasad ciągłości działania, obejmującym określenie ról i odpowiedzialności, nadzór nad planami ciągłości działania oraz działania doskonalące;
i) co najmniej jedna osoba posiada doświadczenie w utrzymaniu lub przeglądzie rozwiązań z zakresu ciągłości działania, obejmującym aktualizację planów oraz uwzględnienie wniosków wynikających z przeprowadzonego ćwiczenia lub rzeczywistego zakłócenia ciągłości działania;
j) co najmniej jedna osoba posiada łącznie:
• doświadczenie w realizacji co najmniej jednej umowy obejmującej wdrożenie lub utrzymanie rozwiązań IT/OT, oraz
• doświadczenie w zakresie wymagań dotyczących dostępu, zarządzania incydentami oraz poziomu świadczenia usług (SLA).

W zakresie wymagania określonego w lit. j) zamawiający wymaga, aby ocena aspektów prawnych była zapewniona przez osobę posiadającą wykształcenie prawnicze i doświadczenie w zakresie umów IT, natomiast ocena aspektów technicznych była zapewniona przez osobę posiadającą doświadczenie w zakresie cyberbezpieczeństwa środowisk IT/OT. Funkcje te może pełnić jedna osoba, pod warunkiem że spełnia łącznie oba wymagania.

W przypadku doświadczenia, o którym mowa w lit. c), opis doświadczenia dotyczącego udziału w autoryzowanej kampanii socjotechnicznej powinien uwzględniać sposób zabezpieczenia przeprowadzonego testu, przy czym wykonawca nie jest zobowiązany do ujawniania wyników kampanii przeprowadzonych na rzecz innych podmiotów.

W przypadku doświadczenia, o którym mowa w lit. d), zamawiający nie wymaga zastosowania określonego narzędzia lub rozwiązania służącego do przeprowadzenia symulacji.

W przypadku doświadczenia, o którym mowa w lit. e), zamawiający nie ustanawia dodatkowej minimalnej wartości zamówienia referencyjnego ani odrębnego wymagania dotyczącego pełnienia funkcji kierownika projektu.

W przypadku doświadczenia, o którym mowa w lit. f), zamawiający nie wymaga, aby osoba posiadała status zewnętrznego pełnomocnika, ani nie wymaga udziału dodatkowego zespołu o określonej liczebności.

> W przypadku doświadczenia, o którym mowa w lit. i), zamawiający nie wymaga udziału odrębnego zespołu całodobowego.
>
> W przypadku doświadczenia, o którym mowa w lit. j), zamawiający nie ustanawia minimalnej wartości umów referencyjnych.
>
> Wymagania określone w lit. a)–j) nie wymagają posiadania dodatkowych certyfikatów, przy czym pozostają w mocy wspólne wymagania dotyczące kwalifikacji i certyfikatów określone w pozostałych warunkach udziału w postępowaniu.

Kryteria oceny do części 1

Czy kryterium cenowe?

TAK

Opis

Sposób oceny ofert: Szczegółowy sposób oceny ofert został podany w pkt 20 Specyfikacji Warunków Zamówienia
Nazwa kryterium: Cena ryczałtowa brutto
Waga: 100% = 100 pkt
Punkty uzyskane za wyżej wymienione kryterium oceny stanowić będą końcową ocenę danej oferty.

Podsumowanie

Oś czasu związana z ogłoszeniem i ofertowaniem

-> 2026-10-06 - data opublikowania

-> 2026-10-21 11:00:00 - termin składania ofert

-> 2026-11 - planowany termin podpisania umowy

Oś czasu realizacji przedmiotów zamówienia

Brak zdefiniowanych etapów dla przedmiotów zamówienia.