Ogłoszenie

Numer

2026-47288-271580

Id

271580

Powstaje w kontekście projektu

KPOD.05.10-IW.06-0001/25 - Cyberbezpieczne Wodociągi

Tytuł

Opracowanie, wdrożenie, przegląd dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa

Warunki zmiany umowy

1. Zamawiający dopuszcza możliwość zmian umowy w stosunku do treści oferty, na podstawie, której dokonano wyboru Wykonawcy w następujących przypadkach:
1) zmiany powszechnie obowiązujących przepisów prawa, których uchwalenie lub zmiana nastąpiły po dniu zawarciu niniejszej umowy, a z których treści wynika konieczność lub zasadność wprowadzenia zmian, mających wpływ na realizację umowy;
2) zmianie nazwy, adresu firmy, spowodowane zmianą formy organizacyjno-prawnej, przekształceniem lub połączeniem z inną firmą;
3) zmianie wynagrodzenia Wykonawcy w przypadku zmiany przez ustawodawcę przepisów dotyczących stawki procentowej należnego podatku VAT;
4) zmian będących następstwem wystąpienia Siły Wyższej, tj. wyjątkowego wydarzenia lub okoliczności, na którą Strona nie ma wpływu, przeciw której Strona nie mogła w racjonalny sposób zabezpieczyć się przed zawarciem umowy, której nie mogła w racjonalny sposób uniknąć lub jej przezwyciężyć;
2. Wszelkie zmiany i uzupełnienia treści umowy mogą być dokonywane wyłącznie za zgodą obydwu stron i stosownie uzasadnione, w formie pisemnej, w postaci aneksu do umowy podpisanego przez obydwie strony pod rygorem nieważności.

Załączniki

Dodane do ogłoszenia w obowiązującej wersji z dn. 2026-03-31
1. Załącznik nr 1 do IWZ- Formularz Cenowo-Ofertowy
2. Załącznik nr 2 do IWZ- Oświadczenie
3. Załącznik nr 3 do IWZ- Wykaz osób
4. Załącznik nr 4 do IWZ- Wykaz usług

5. Załącznik nr 5 do IWZ- Opis Przedmiotu Zamówienia
6. Załącznik nr 6 do IWZ- Projekt umowy
7. Istotne Warunki Zamówienia

Czy dopuszczalna oferta częściowa?

NIE

Data opublikowania ogłoszenia

2026-03-31

Data ostatniej zmiany

2026-03-31

Termin składania ofert

2026-04-15 12:00:00

Planowany termin podpisania umowy

2026-04

Dane adresowe ogłoszeniodawcy

> Miejskie Przedsiębiorstwo Wodociągów i Kanalizacji
> Spółka z ograniczoną odpowiedzialnością w Lubinie
> Rzeźnicza 1
> 59-300 Lubin
> NIP: 6920212117

Osoby do kontaktu

> Magdalena Cirko
> tel.: -
> e-mail: zamowieniapubliczne@mpwik.lubin.pl

> Anna Bartecka
> tel.: -
> e-mail: zamowieniapubliczne@mpwik.lubin.pl

Części zamówienia

Część: 1

Tytuł części 1

Opracowanie i wdrożenie dokumentacji SZBI oraz szkolenia

Czy dopuszczalne oferty wariantowe

NIE

Przedmioty zamówienia do części 1

Typ

Usługa

Podkategoria

Usługi IT

Opis

1.Przedmiotem zamówienia jest świadczenie usług z zakresu cyberbezpieczeństwa, obejmujących:
1) opracowanie i wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) wraz z szacowaniem ryzyka zgodnym z ISO/IEC 27005;
2) przeprowadzenie praktycznych szkoleń z zakresu cyberbezpieczeństwa dla pracowników i kadry kierowniczej Zamawiającego.
2. Wykonawca oświadcza, że usługi będą świadczone przez osoby posiadające kwalifikacje i certyfikaty wymagane przy realizacji przedmiotu zamówienia.
3. Szczegółowy zakres przedmiotu zamówienia został określony w Załączniku nr 5 do IWZ.

Okres gwarancji

Wykonawca udziela gwarancji na prawidłowość i kompletność dostarczonej dokumentacji SZBI przez okres 12 miesięcy od dnia podpisania protokołu końcowego odbioru.

Kody CPV

72220000-3 Usługi doradcze w zakresie systemów i doradztwo techniczne
72246000-1 Usługi doradcze w zakresie systemów
80510000-2 Usługi szkolenia specjalistycznego

Miejsca realizacji

adres

Kraj **Województwo**

Polska

dolnośląskie

Powiat

lubiński

Gmina

Lubin

Miejscowość

Lubin

Warunki, jakie musi spełniać oferent

Typ

Osoby zdolne do wykonania zamówienia

Opis

Zamawiający uzna, że Wykonawca spełnia warunek w zakresie dysponowania odpowiednimi osobami zdolnymi do wykonywania zamówienia, jeżeli Wykonawca wykaże, że: dysponuje zespołem skierowanym do realizacji przedmiotu zamówienia składającym się z co najmniej 3 osób, przy czym skład ten powinien obejmować:
1.1. minimum 3 osoby posiadające ważne certyfikaty audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 lub równoważnej, wydane przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób;
1.2. minimum 2 osoby posiadające wiedzę i doświadczenie w obszarze audytów systemów zarządzania bezpieczeństwem informacji przy spełnieniu wymagań dla audytorów IRCA, CQI, potwierdzonych certyfikatem lub równoważnym dokumentem ukończenia kursu Information Security Management Systems (ISMS) Auditor;
1.3. minimum 1 osobę w zespole posiadającą wiedzę i doświadczenie w zakresie wdrażania systemów zarządzania bezpieczeństwem informacji zgodnych z normą ISO 27001 lub równoważnych standardów o zbliżonym poziomie jakości. Wymagane jest potwierdzenie kwalifikacji ważnym certyfikatem lub równoważnym dokumentem ukończenia szkolenia w tym obszarze. Ponadto osoba ta musi posiadać doświadczenie w realizacji wdrożeń systemu zarządzania bezpieczeństwem informacji realizowanych w co najmniej 5 podmiotach publicznych;
1.4. minimum 1 osobę z kwalifikacjami w zakresie audytowania systemów zarządzania ciągłością działania, potwierdzonymi spełnieniem wymagań dla audytorów wiodących systemu zarządzania ciągłością działania zgodnego z normą PN-EN ISO 22301, lub równoważną, potwierdzone certyfikatem dla audytora wiodącego systemu zarządzania ciągłością działania zgodnego z normą PN-EN ISO 22301 po zdaniu egzaminu;
1.5. minimum 1 osobę posiadającą wiedzę i doświadczenie w zakresie wdrażania systemu

zarządzania ciągłością działania wg ISO 22301 potwierdzoną ważnym certyfikatem lub równoważnym dokumentem ukończenia szkolenia w tym zakresie;
1.6. przynajmniej 2 osoby posiadające kompetencje w zakresie audytowania systemów zarządzania jakością przy spełnieniu wymagań dla audytorów wewnętrznych systemu zarządzania jakością zgodnego z normą PN-EN ISO 9001 lub wymagań równoważnych, tj. określonych na nie niższym poziomie jakości, potwierdzone ważnym certyfikatem dla audytora wewnętrznego systemu zarządzania jakością zgodnego z normą PN-EN ISO 9001 po zdaniu egzaminu;
1.7. minimum 2 osoby, które posiadają kwalifikacje potwierdzone ukończeniem studiów podyplomowych z zakresu ochrony danych osobowych oraz co najmniej 8-letnie doświadczenie zawodowe na stanowisku Inspektora Ochrony Danych lub Administratora Bezpieczeństwa Informacji;
1.8. minimum 2 osoby, które brały udział w realizacji co najmniej 2 projektów związanych z zarządzaniem ryzykiem w zakresie bezpieczeństwa informacji, w tym co najmniej 1 projekcie zrealizowanego zgodnie z normą ISO 27005 lub równoważną;
1.9. minimum 1 osobę posiadającą wiedzę oraz praktyczne umiejętności w zarządzaniu ryzykiem w obszarze ochrony informacji. Kwalifikacje tej osoby powinny być poświadczone ważnym certyfikatem lub równoważnym dokumentem ukończenia szkolenia w tym zakresie;
1.10. minimum 1 osobę, która posiada doświadczenie w prowadzeniu szkoleń i zrealizowała minimum 10 szkoleń dotyczących cyberbezpieczeństwa, bezpieczeństwa informacji lub ochrony danych, skierowanych do podmiotów publicznych;
1.11. minimum 1 osobę w zespole posiadającą wiedzę na temat wymagań określonych w Ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Kwalifikacje te muszą być potwierdzone ważnym certyfikatem lub równoważnym dokumentem ukończenia odpowiedniego szkolenia w tym zakresie;
1.12. minimum 1 osobę w zespole posiadającą wiedzę z zakresu zarządzania cyberbezpieczeństwem, potwierdzoną aktualnym certyfikatem lub równoważnym dokumentem ukończenia szkolenia w tym obszarze;
1.13. minimum 1 osobę, która ukończyła techniczne studia wyższe w dziedzinie cyberbezpieczeństwa i posiada tytuł inżyniera, co powinno być udokumentowane dyplomem ukończenia studiów wyższych;
1.14. minimum 1 osobę w zespole posiadającą specjalistyczną wiedzę i umiejętności w zakresie administrowania sieciami teleinformatycznymi, potwierdzone aktualnym certyfikatem lub równoważnym dokumentem ukończenia szkolenia w tym zakresie;
1.15. minimum 1 osobę, która powinna odbyć specjalistyczne szkolenie z zakresu cyberbezpieczeństwa, zgodnie z normami ISO 27001, 22301 oraz przepisami RODO. Wymagane jest potwierdzenie ukończenia szkolenia certyfikatem lub równoważnym dokumentem;
1.16. minimum 1 osobę posiadającą wiedzę i doświadczenie w zakresie zapewnienia cyberbezpieczeństwa infrastruktury Active Directory, potwierdzone ważnym certyfikatem lub równoważnym dokumentem ukończenia szkolenia w tym zakresie;

1.17. minimum 1 osobę posiadającą wiedzę i doświadczenie w zakresie białego wywiadu (OSINT) potwierdzone ważnym certyfikatem lub równoważnym dokumentem ukończenia szkolenia w tym zakresie;
1.18. minimum 1 osobę posiadającą wiedzę i doświadczenie w zakresie sztucznej inteligencji, potwierdzone ważnym certyfikatem lub równoważnym dokumentem ukończenia szkolenia w tym zakresie.
Zamawiający dopuszcza łączenie stanowisk oraz uprawnień przez osoby wskazane przez Wykonawcę w celu spełnienia warunku udziału w postępowaniu dot. osób.

Typ

Potencjał techniczny

Opis

Zamawiający uzna, że Wykonawca spełnia warunek w zakresie dysponowania odpowiednim potencjałem technicznym, jeżeli Wykonawca wykaże, że wykonał należycie w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie co najmniej:
1.1. 3 audyty bezpieczeństwa systemów teleinformatycznych, w tym co najmniej jeden z testami penetracyjnymi, na rzecz podmiotów realizujących zadania publiczne, z których każdy miał wartość nie mniejszą niż 50 000,00 zł brutto, co potwierdzono stosownymi referencjami.
1.2. 4 inne audyty cyberbezpieczeństwa (niewskazane w pkt. 1.1. i 1.3.) dla podmiotów realizujących zadania publiczne, z których każdy miał wartość nie mniejszą niż 20 000,00 zł brutto, co zostało udokumentowane referencjami.
1.3. 15 innych audytów bezpieczeństwa informacji (niewskazanych w pkt. 1.1. i 1.2.).
1.4. 2 usługi przeprowadzenia szkoleń z zakresu cyberbezpieczeństwa dla podmiotów realizujących zadania publiczne, z których każda miała wartość nie mniejszą niż 20 000,00 zł brutto, co zostało udokumentowane referencjami.
1.5. opracował dokumentację systemu zarządzania bezpieczeństwem informacji dla minimum 5 podmiotów realizujących zadania publiczne, co potwierdzono stosownymi referencjami.
1.6. zrealizował co najmniej 2 projekty dotyczące szacowania ryzyka związanego z bezpieczeństwem danych w systemach informatycznych dla podmiotów realizujących zadania publiczne, co zostało potwierdzone stosownymi referencjami.

Typ

Dodatkowe warunki udziału

Opis

1.O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy nie są powiązani kapitałowo lub osobowo z Zamawiającym.

> 2. Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między Zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Zamawiającego lub osobami wykonującymi w imieniu Zamawiającego czynności związane z przeprowadzeniem procedury wyboru Wykonawcy a Wykonawcą, polegające w szczególności na:
> 2.1. uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej;
> 2.2. posiadaniu co najmniej 10 % udziałów lub akcji (o ile niższy próg nie wynika z przepisów prawa), pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika;
> 2.3. pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa lub powinowactwa w linii bocznej do drugiego stopnia lub w stosunku przysposobienia, opieki lub kurateli, pozostawaniu we wspólnym pożyciu z wykonawcą, jego zastępcą prawnym lub członkami organów zarządzających lub organów nadzorczych wykonawców wspólnie ubiegających się o udzielenie zamówienia;
> 2.4. pozostawaniu z wykonawcą w takim stosunku prawnym lub faktycznym, że istnieje uzasadniona wątpliwość co do mojej bezstronności lub niezależności w związku z przedmiotowym postępowaniem o udzielenie zamówienia. W celu uniknięcia konfliktu interesów, w przypadku beneficjenta, który nie jest zamawiającym w rozumieniu Pzp, zamówienia nie mogą być udzielane podmiotom powiązanym z nim osobowo lub kapitałowo, z wyłączeniem zamówień sektorowych i zamówień określonych w sekcji 3.2.1 pkt 2 lit. i Wytycznych kwalifikowalności.

Kryteria oceny do części 1

Czy kryterium cenowe?

TAK

Opis

Kryterium oceny ofert będzie stanowiła najniższa cena ofertowa brutto za świadczenie usług z zakresu cyberbezpieczeństwa:
1. opracowanie i wdrożenie dokumentacji SZBI wraz z szacowaniem ryzyka.
2. przeprowadzenie praktycznych szkoleń dla pracowników i kadry kierowniczej.

Podsumowanie

Oś czasu związana z ogłoszeniem i ofertowaniem

-> 2026-03-31 - data opublikowania

-> 2026-04-15 12:00:00 - termin składania ofert

-> 2026-04 - planowany termin podpisania umowy

Oś czasu realizacji przedmiotów zamówienia

Brak zdefiniowanych etapów dla przedmiotów zamówienia.