Ogłoszenie o zmianie ogłoszenia
Wdrożenie zaawansowanych rozwiązań cyberbezpieczeństwa w ZWiK Wierzbica w ramach projektu „Cyberbezpieczne Wodociągi”

SEKCJA I - ZAMAWIAJĄCY

1.1.) Nazwa zamawiającego: GMINA WIERZBICA -ZAKŁAD WODOCIĄGÓW I KANALIZACJI W WIERZBICY

1.3.) Krajowy Numer Identyfikacyjny: REGON 672773546

1.4.) Adres zamawiającego:

1.4.1.) Ulica: ul. Kościuszki 73

1.4.2.) Miejscowość: Wierzbica

1.4.3.) Kod pocztowy: 26-680

1.4.4.) Województwo: mazowieckie

1.4.5.) Kraj: Polska

1.4.6.) Lokalizacja NUTS 3: PL912 - Warszawski wschodni

1.4.9.) Adres poczty elektronicznej: biuro@zwik-wierzbica.pl

1.4.10.) Adres strony internetowej zamawiającego: https://samorzad.gov.pl/web/maz-wierzbica

1.5.) Rodzaj zamawiającego: Zamawiający sektorowy - art. 5 ust. 1 pkt 1 - gospodarka wodna

1.6.) Przedmiot działalności zamawiającego: Środowisko

SEKCJA II – INFORMACJE PODSTAWOWE

SEKCJA III ZMIANA OGŁOSZENIA

3.1.) Nazwa zmienianego ogłoszenia:
Ogłoszenie o zamówieniu

3.2.) Numer zmienianego ogłoszenia w BZP: 2026/BZP 00394391

3.3.) Identyfikator ostatniej wersji zmienianego ogłoszenia: 01

3.4.) Identyfikator sekcji zmienianego ogłoszenia:
SEKCJA V - KWALIFIKACJA WYKONAWCÓW

3.4.1.) Opis zmiany, w tym tekst, który należy dodać lub zmienić:
5.4. Nazwa i opis warunków udziału w postępowaniu

Przed zmianą:
Dla Części Pierwszej:
1. w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, wykonał należycie co najmniej dwie dostawy sprzętu informatycznego, obejmującego: dostawę, wdrożenie oraz utrzymanie urządzenia firewall, przy czym:
- obie dostawy obejmujące ww. zakres były o wartości co najmniej 500.000,00 zł brutto każda;
- jedna z dostaw obejmująca ww. zakres zrealizowana była na rzecz podmiotu wchodzącego w skład infrastruktury krytycznej w rozumieniu przepisów ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. Przez podmiot infrastruktury krytycznej Zamawiający rozumie operatora infrastruktury krytycznej, o którym mowa w art. 3 pkt 2 ustawy o zarządzaniu kryzysowym.

Uwaga:
Jeżeli Wykonawca powołuje się na doświadczenie w realizacji dostaw wykonywanych wspólnie z innymi wykonawcami, należy wykazać dostawę (zakres), w której Wykonawca bezpośrednio uczestniczył.

Do przeliczenia wszystkich wartości finansowych, a występujących w innych walutach niż PLN Wykonawca zastosuje średni kurs Narodowego Banku Polskiego (NBP) opublikowany w dniu ukazania się ogłoszenia o niniejszym zamówieniu na stronie internetowej prowadzonego postępowania. Średnie kursy walut dostępne są na stronie internetowej Narodowego Banku Polskiego pod następującym adresem: http://www.nbp.pl/.

2. Wykonawca wskaże osoby do wykonania niniejszego zamówienia, legitymujące się kwalifikacjami zawodowymi, uprawnieniami, doświadczeniem i wykształceniem odpowiednim do funkcji, które zostaną im powierzone, które muszą być dostępne na etapie realizacji zamówienia, spełniające następujące wymagania:

- dwie osoby, które będą pełniły funkcję specjalisty/eksperta ds. wdrożenia rozwiązań IT, posiadające doświadczenie w co najmniej trzech projektach, których przedmiotem było wdrożenie mechanizmów i środków zwiększających odporność na ataki z cyberprzestrzeni, przy czym minimum jedna z wyżej wymienionych osób ma obowiązek legitymować się:
- certyfikatem CISSP - Certified Information Systems Security Professional lub równoważny. Za równoważny uznaje się certyfikat wystawiany przez niezależną instytucję posiadającą uprawnienia do potwierdzania kompetencji w obszarze bezpieczeństwa systemów informatycznych. Certyfikat równoważny musi dotyczyć tego samego obszaru kwalifikacji, a jego uzyskanie musi wiązać się z przejściem procedury certyfikacyjnej takiej samej jak w przypadku certyfikatu porównywanego;
lub
- certyfikatrm CISA – Certified Information Systems Auditor lub certyfikat równoważny. Za równoważny uznaje się certyfikat wystawiany przez niezależną instytucję posiadającą uprawnienia do potwierdzania kompetencji w obszarze audytu systemów informatycznych oraz kontroli i zarządzania IT. Certyfikat równoważny musi dotyczyć tego samego obszaru kwalifikacji, a jego uzyskanie musi wiązać się z przejściem procedury certyfikacyjnej obejmującej w szczególności weryfikację wiedzy w formie egzaminu oraz spełnienie wymogów dotyczących doświadczenia zawodowego, analogicznie jak w przypadku certyfikatu porównywanego;
oraz
- certyfikatem w stopniu inżyniera, wystawionym przez producenta oferowanego rozwiązania do tworzenia kopii zapasowych.

Dla Części Drugiej:
1) w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, wykonał należycie co najmniej jedną dostawę agregatów prądotwórczych wraz z usługą projektu oraz wykonania przyłącza elektrycznego do agregatu prądotwórczego o wartości co najmniej 80.000,00 zł brutto.

Do przeliczenia wszystkich wartości finansowych, a występujących w innych walutach niż PLN Wykonawca zastosuje średni kurs Narodowego Banku Polskiego (NBP) opublikowany w dniu ukazania się ogłoszenia o niniejszym zamówieniu na stronie internetowej prowadzonego postępowania. Średnie kursy walut dostępne są na stronie internetowej Narodowego Banku Polskiego pod następującym adresem: http://www.nbp.pl/.

Dla Części Trzeciej:
1. Wykonawca wykaże, że dysponuje lub będzie dysponował osobami zdolnymi do realizacji zamówienia, które będą uczestniczyć w wykonywaniu zamówienia, przy czym co najmniej:
a) audytorem zewnętrznym* posiadającym przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz. 1999 z późn. zm.)
lub
b) audytorem wewnętrznym posiadającym przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz. 1999 z późn. zm)
lub
c) będącego audytorem zewnętrznym* systemu zarządzania bezpieczeństwem informacji według normy PN-ISO/IEC 27001;
oraz
2. 1 (jednym) audytorem wiodącym według normy PN-ISO/IEC 27001 posiadającym doświadczenie w realizacji co najmniej jednej usługi polegającej na wykonaniu audytu cyberbezpieczeństwa zgodnie z normą PN-ISO/IEC 27001 lub zapisami z §20 ust. 2 pkt 14 rozporządzenia w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2017 poz. 2247 ze zm.).

* audytor zewnętrzny – za audytora zewnętrznego uznaje się audytora niepowiązanego z Zamawiającym żadnym stosunkiem prawnym.

Zamawiający nie dopuszcza wskazania jednego audytora celem wykazania warunków określonych w pkt a) – d) powyżej.

Dla Części Czwartej:
1. Wykonawca wykaże, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wykonał co najmniej:
a. 2 usługi polegające na opracowaniu i wdrożeniu Polityki Bezpieczeństwa Informacji lub przygotowaniu i wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji, w skład którego wchodzi kompletna dokumentacja Polityki Bezpieczeństwa Informacji.
2. Wykonawca wykaże, że dysponuje lub będzie dysponował osobami zdolnymi do realizacji zamówienia, które będą uczestniczyć w wykonywaniu zamówienia, przy czym co najmniej:

a) 1 osobą będącą audytorem wiodącym posiadającym uprawnienia według normy PN-ISO/IEC 27001 oraz posiadającą co najmniej 3-letnie doświadczenie w zakresie opracowywania i wdrażania Polityki Bezpieczeństwa Informacji lub Systemu Zarządzania Bezpieczeństwem Informacji, zgodnie z wymaganiami normy PN-ISO/IEC 27001.

Dla Części Piątej:
1. Wykonawca wykaże, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie:
a. posiada minimum 2-letnie doświadczenie w przygotowaniu i przeprowadzeniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń;
b. przeprowadził co najmniej 5 szkoleń z cyberbezpieczeństwa;
2. Wykonawca wykaże, że dysponuje lub będzie dysponował osobami zdolnymi do realizacji zamówienia, które będą uczestniczyć w wykonywaniu zamówienia, przy czym co najmniej:
a. 2 osobami, które przeprowadziły co najmniej 5 szkoleń* (każda z nich) z obszaru cyberbezpieczeństwa, w tym 3 szkolenia dedykowane kadrze zarządzającej i informatykom.

*Zamawiający dopuszcza, żeby szkolenia, które realizowały osoby wskazane przez wykonawcę do realizacji zamówienia były to te same szkolenia, jeśli jednocześnie wykaże (np. poprzez referencje), że dwóch szkoleniowców prowadziło to samo szkolenie.

Po zmianie:
Dla Części Pierwszej:
1. w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, wykonał należycie co najmniej dwie dostawy sprzętu informatycznego, obejmującego: dostawę, wdrożenie oraz utrzymanie urządzenia firewall, przy czym:
- obie dostawy obejmujące ww. zakres były o wartości co najmniej 500.000,00 zł brutto każda;
- jedna z dostaw obejmująca ww. zakres zrealizowana była na rzecz podmiotu wchodzącego w skład infrastruktury krytycznej w rozumieniu przepisów ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. Przez podmiot infrastruktury krytycznej Zamawiający rozumie operatora infrastruktury krytycznej, o którym mowa w art. 3 pkt 2 ustawy o zarządzaniu kryzysowym.

Uwaga:
Jeżeli Wykonawca powołuje się na doświadczenie w realizacji dostaw wykonywanych wspólnie z innymi wykonawcami, należy wykazać dostawę (zakres), w której Wykonawca bezpośrednio uczestniczył.

Do przeliczenia wszystkich wartości finansowych, a występujących w innych walutach niż PLN Wykonawca zastosuje średni kurs Narodowego Banku Polskiego (NBP) opublikowany w dniu ukazania się ogłoszenia o niniejszym zamówieniu na stronie internetowej prowadzonego postępowania. Średnie kursy walut dostępne są na stronie internetowej Narodowego Banku Polskiego pod następującym adresem: http://www.nbp.pl/.

2. Wykonawca wskaże osoby do wykonania niniejszego zamówienia, legitymujące się kwalifikacjami zawodowymi, uprawnieniami, doświadczeniem i wykształceniem odpowiednim do funkcji, które zostaną im powierzone, które muszą być dostępne na etapie realizacji zamówienia, spełniające następujące wymagania:

- dwie osoby, które będą pełniły funkcję specjalisty/eksperta ds. wdrożenia rozwiązań IT, posiadające doświadczenie w co najmniej trzech projektach, których przedmiotem było wdrożenie mechanizmów i środków zwiększających odporność na ataki z cyberprzestrzeni, przy czym minimum jedna z wyżej wymienionych osób ma obowiązek legitymować się:
- certyfikatem CISSP - Certified Information Systems Security Professional lub równoważny. Za równoważny uznaje się certyfikat wystawiany przez niezależną instytucję posiadającą uprawnienia do potwierdzania kompetencji w obszarze bezpieczeństwa systemów informatycznych. Certyfikat równoważny musi dotyczyć tego samego obszaru kwalifikacji, a jego uzyskanie musi wiązać się z przejściem procedury certyfikacyjnej takiej samej jak w przypadku certyfikatu porównywanego; lub
- certyfikatrm CISA – Certified Information Systems Auditor lub certyfikat równoważny. Za równoważny uznaje się certyfikat wystawiany przez niezależną instytucję posiadającą uprawnienia do potwierdzania kompetencji w obszarze audytu systemów informatycznych oraz kontroli i zarządzania IT. Certyfikat równoważny musi dotyczyć tego samego obszaru kwalifikacji, a jego uzyskanie musi wiązać się z przejściem procedury certyfikacyjnej obejmującej w szczególności weryfikację wiedzy w formie egzaminu oraz spełnienie wymogów dotyczących doświadczenia zawodowego, analogicznie jak w przypadku certyfikatu porównywanego.

Dla Części Drugiej:
1) w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, wykonał należycie co najmniej jedną dostawę agregatów prądotwórczych wraz z usługą projektu oraz wykonania przyłącza elektrycznego do agregatu prądotwórczego o wartości co najmniej 80.000,00 zł brutto.

Do przeliczenia wszystkich wartości finansowych, a występujących w innych walutach niż PLN Wykonawca zastosuje średni kurs Narodowego Banku Polskiego (NBP) opublikowany w dniu ukazania się ogłoszenia o niniejszym zamówieniu na stronie

internetowej prowadzonego postępowania. Średnie kursy walut dostępne są na stronie internetowej Narodowego Banku Polskiego pod następującym adresem: http://www.nbp.pl/.

Dla Części Trzeciej:
1. Wykonawca wykaże, że dysponuje lub będzie dysponował osobami zdolnymi do realizacji zamówienia, które będą uczestniczyć w wykonywaniu zamówienia, przy czym co najmniej:
a) audytorem zewnętrznym* posiadającym przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz. 1999 z późn. zm.)
lub
b) audytorem wewnętrznym posiadającym przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz. 1999 z późn. zm)
lub
c) będącego audytorem zewnętrznym* systemu zarządzania bezpieczeństwem informacji według normy PN-ISO/IEC 27001;
oraz
2. 1 (jednym) audytorem wiodącym według normy PN-ISO/IEC 27001 posiadającym doświadczenie w realizacji co najmniej jednej usługi polegającej na wykonaniu audytu cyberbezpieczeństwa zgodnie z normą PN-ISO/IEC 27001 lub zapisami z §20 ust. 2 pkt 14 rozporządzenia w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2017 poz. 2247 ze zm.).

* audytor zewnętrzny – za audytora zewnętrznego uznaje się audytora niepowiązanego z Zamawiającym żadnym stosunkiem prawnym.

Zamawiający nie dopuszcza wskazania jednego audytora celem wykazania warunków określonych w pkt a) – d) powyżej.

Dla Części Czwartej:
1. Wykonawca wykaże, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wykonał co najmniej:
a. 2 usługi polegające na opracowaniu i wdrożeniu Polityki Bezpieczeństwa Informacji lub przygotowaniu i wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji, w skład którego wchodzi kompletna dokumentacja Polityki Bezpieczeństwa Informacji.
2. Wykonawca wykaże, że dysponuje lub będzie dysponował osobami zdolnymi do realizacji zamówienia, które będą uczestniczyć w wykonywaniu zamówienia, przy czym co najmniej:
a) 1 osobą będącą audytorem wiodącym posiadającym uprawnienia według normy PN-ISO/IEC 27001 oraz posiadającą co najmniej 3-letnie doświadczenie w zakresie opracowywania i wdrażania Polityki Bezpieczeństwa Informacji lub Systemu Zarządzania Bezpieczeństwem Informacji, zgodnie z wymaganiami normy PN-ISO/IEC 27001.

Dla Części Piątej:
1. Wykonawca wykaże, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie:
a. posiada minimum 2-letnie doświadczenie w przygotowaniu i przeprowadzeniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń;
b. przeprowadził co najmniej 5 szkoleń z cyberbezpieczeństwa;
2. Wykonawca wykaże, że dysponuje lub będzie dysponował osobami zdolnymi do realizacji zamówienia, które będą uczestniczyć w wykonywaniu zamówienia, przy czym co najmniej:
a. 2 osobami, które przeprowadziły co najmniej 5 szkoleń* (każda z nich) z obszaru cyberbezpieczeństwa, w tym 3 szkolenia dedykowane kadrze zarządzającej i informatykom.

*Zamawiający dopuszcza, żeby szkolenia, które realizowały osoby wskazane przez wykonawcę do realizacji zamówienia były to te same szkolenia, jeśli jednocześnie wykaże (np. poprzez referencje), że dwóch szkoleniowców prowadziło to samo szkolenie.

3.4.) Identyfikator sekcji zmienianego ogłoszenia:
SEKCJA VIII - PROCEDURA

3.4.1.) Opis zmiany, w tym tekst, który należy dodać lub zmienić:
8.1. Termin składania ofert

Przed zmianą:
2026-08-26 10:00

Po zmianie:
2026-08-28 10:00

3.4.1.) Opis zmiany, w tym tekst, który należy dodać lub zmienić:
8.3. Termin otwarcia ofert

Przed zmianą:
2026-08-26 10:10

Po zmianie:
2026-08-28 10:10

3.4.1.) Opis zmiany, w tym tekst, który należy dodać lub zmienić:
8.4. Termin związania ofertą

Przed zmianą:
2026-09-24

Po zmianie:
2026-09-26