ZAPYTANIE OFERTOWE

na wykonanie **DIAGNOZY CYBERBEZPIECZEŃSTWA**

w ramach projektu pn. "Cyfrowa Gmina" realizowanego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Oś V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia- REACT-EU, Działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia:

I. Zamawiający:

Gmina Raciążek
87-721 Raciążek
NIP: 891-15-55-882
Tel.: 54 283 18-85
E-mail: gmina@raciazek.pl

II. Tryb postępowania:

1. Postępowanie o udzielenie zamówienia publicznego jest wyłączone z obowiązku stosowania ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t. j. Dz.U. 2021 poz. 1129 z późn. zm.) na podstawie art. 2 ust. 1 pkt 1.
2. Postępowanie o udzielenie zamówienia publicznego prowadzone jest w oparciu o Zarządzenie Nr 58/2022 Wójta Gminy Raciążek z dnia 31 grudnia 2022 r. w sprawie ustalenia „Procedur udzielana zamówień publicznych, których wartość szacunkowa netto nie przekracza kwoty 130000,00 zł netto w urzędzie gminy Raciążek.

III. Opis przedmiotu zamówienia:

1. Przeprowadzenie diagnozy cyberbezpieczeństwa w ramach projektu „Cyfrowa Gmina" w Urzędzie Gminy Raciążek zgodnie z zakresem oraz formularzem stanowiącym obowiązujący na dzień wykonywania audytu załącznik nr 8 do Regulaminu Konkursu Grantowego Cyfrowa Gmina zakończonego raportem, opublikowanego na stronie Centrum Projektów Polska Cyfrowa pod adresem https://www.gov.pl/web/cppc/cyfrowa-gmina.
2. Zamawiający nie dopuszcza wykonania diagnozy cyberbezpieczeństwa w sposób zdalny. Badanie zabezpieczeń, w tym przeprowadzenie wszelakich testów penetracyjnych sieci LAN, diagnozy cyberbezpieczeństwa, podatności systemów, wykonawca musi wykonać na miejscu w siedzibie Zamawiającego.
3. Szczegółowy zakres przedmiotu zamówienia zawiera formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa stanowiący załącznik nr 6 do zapytania ofertowego.
4. Po przeprowadzeniu diagnozy, Wykonawca zobligowany jest do przekazania wypełnionego i podpisanego elektronicznie formularza diagnozy (przeprowadzonej przez osobę posiadającą uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu) Zamawiającemu oraz dostarczenia wersji papierowej. Wykonawca poza formularzem przekaże dokumentację składową na podstawie której został opracowany załącznik diagnozy cyberbezpieczeństwa. Zamawiający ma na myśli dokumentację szczegółową kontrolowanych punktów, systemów, czy innych elementów składowych wpływających na ocenę końcową

danej kategorii wprowadzoną do formularza diagnozy. Wykonawca przekaże również zestawienie , na podstawie którego Zamawiający punkt po punkcie będzie mógł dokonać prac naprawczych/wdrożeniowych podnoszących bezpieczeństwo systemów oraz dopracowanie procedur postępowania.

IV. Warunki udziału Wykonawcy w postępowaniu:

1. Diagnoza cyberbezpieczeństwa musi zostać przeprowadzona przez osobę posiadającą uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Wykaz certyfikatów wskazanych w ww. rozporządzeniu znajduje się poniżej:
   1) Certified Internal Auditor (CIA),
   2) Certified Information System Auditor (CISA),
   3) Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany 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,
   4) Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób,
   5) Certified Information Security Manager (CISM),
   6) Certified in Risk and Information Systems Control (CRISC),
   7) Certified in the Govemance of Enterprise IT (CGEIT)
   8) Certified Information Systems Security Professional (CISSP),
   9) Systems Security Certified Practitioner (SSCP),
   10) Certified Reliability Professional,
   11) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.
2. Wykonawca posiada potencjał techniczny i osobowy niezbędny do wykonania zamówienia. Wykonawca złoży w tym zakresie oświadczenie stanowiące załącznik nr 2 do oferty.
3. Wykonawca posiada doświadczenie w wykonywaniu audytów wynikających z Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. Wykonawca złoży w tym zakresie oświadczenie będące załącznikiem nr 3 do oferty wraz z dokumentami potwierdzającymi przeprowadzenie minimum 1 diagnozy cyberbezpieczeństwa w ramach programu Cyfrowa Gmina oraz zrealizowania co najmniej 3 audytów bezpieczeństwa w jednostkach administracji publicznej o podobnym zakresie w ostatnich 3 latach przed złożeniem oferty. Wykonawcy, którzy nie wykażą spełnienia warunków udziału w postępowaniu podlegać będą wykluczeniu z udziału w postępowaniu. Ofertę Wykonawcy wykluczonego uznaje się za odrzuconą.
4. Wykonawca zobowiązany jest przekazać dane osoby, która będzie wykonywała diagnozę wraz z dokumentem potwierdzającym posiadanie przez niego certyfikatu uprawniającego do przeprowadzeniu audytu, o którym mowa w Rozporządzeniu Ministra Cyfryzacji z 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu -załącznik nr 4 do zapytania.
5. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu na podstawie art.7 ust. 1 ustawy z dnia 13 kwietnia 2022 roku o szczególnych rozwiązaniach w zakresie przeciwdziałania wspierania agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz.U. poz. 835) - załącznik nr 5 do zapytania.

V. Kryteria i sposób oceny oferty:

1. Przy wyborze oferty do realizacji Zamawiający będzie się kierował kryterium: Cena-100%.
2. Cenę za wykonanie zamówienia należy podać w formularzu oferty.
3. Cena winna obejmować wszelkie koszty niezbędne do zrealizowania zamówienia. Wykonawca sporządzając ofertę powinien przewidzieć wszelkie okoliczności mogące mieć wpływ na cenę.

VI. Termin i miejsce realizacji zamówienia:

Wykonawca jest zobowiązany wykonać zamówienie nie później niż do **15 września 2022 roku** w siedzibie Zamawiającego: ul. Wysoka 4, 87-721 Raciążek

VII. Sposób przygotowania oferty:

1. Kompletny, wypełniony formularz ofertowy, podpisany przez osobę upoważnioną do reprezentacji Wykonawcy stanowiący załącznik nr 1;
2. Kompletne, wypełnione oświadczenie stanowiące załącznik nr 2;
3. Kompletne, wypełnione oświadczenie stanowiące załącznik nr 3;
4. Kompletne, wypełnione oświadczenie stanowiące załącznik nr 4;
5. Kompletne, wypełnione oświadczenie stanowiące załącznik nr 5;
6. Dokumenty potwierdzające wymagane kwalifikacje do przeprowadzenia diagnozy cyberbezpieczeństwa;
7. Referencje potwierdzające prawidłowe wykonanie diagnozy cyberbezpieczeństwa lub audytu.
8. Podpisana klauzula informacyjna RODO- załącznik nr 7.

Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.

VIII. Miejsce i termin składania ofert:

1. Termin składania ofert 16.08.2022r. do godz. 9:00,

2. Ofertę cenową sporządzoną w języku polskim należy złożyć:

a) pisemnie w siedzibie Zamawiającego lub przesłać na adres: ul. Wysoka 4, 87-721 Raciążek w zamkniętej kopercie z dopiskiem: OFERTA: „Przeprowadzenie diagnozy cyberbezpieczeństwa w ramach projektu Cyfrowa Gmina" NIE OTWIERAĆ PRZED 16.08.2022 r. godz. 9:00 lub

b) mailem na adres poczty elektronicznej: g m i n a @ r a c i a z e k . p l (skan podpisanej oferty).

3. Oferty złożone po terminie bądź w inny sposób nie będą rozpatrywane.

IX. Termin związania ofertą:

1. Wykonawca pozostaje związany złożoną ofertą przez okres 30 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

2. Wykonawca samodzielnie lub na wniosek Zamawiającego może przedłużyć termin związania ofertą.

X. Postanowienia końcowe:

1. Zamawiający zastrzega sobie prawo odstąpienia, bądź unieważnienia zapytania ofertowego bez podania przyczyny w przypadku zaistnienia okoliczności nieznanych Zamawiającemu w dniu publikacji niniejszego zapytania ofertowego.

2. Zapytanie może zostać zmienione przed upływem terminu składania ofert przewidzianym w zapytaniu ofertowym. Zmiana zapytania oraz treść pytań wraz z wyjaśnieniami zostanie opublikowana na stronie: https://bazakonkurencvinosci.funduszeeuropeiskie.gov.pl.

3. Jednostki samorządu terytorialnego biorące udział w projekcie "Cyfrowa Gmina" są zobowiązane do przeprowadzenia diagnozy cyberbezpieczeństwa będącej przedmiotem niniejszego zamówienia. Niezwłocznie po jej przeprowadzeniu, jej wyniki mają być przekazane przez Zamawiającego do Naukowej i Akademickiej Sieci Komputerowej-Państwowego Instytutu Badawczego (NASK) za pośrednictwem platformy ePUAP. Dane z diagnozy przekazane przez JST do NASK posłużą do opracowania raportu na temat stanu bezpieczeństwa systemów jednostek samorządowych. Wykonawca jest zobowiązany mieć na uwadze w/w cel przeprowadzenia diagnozy i jej przeznaczenie.

XI. Załączniki:

Załącznik nr 1 – Formularz ofertowy;
Załącznik nr 2 – Oświadczenie o posiadaniu niezbędnego do wykonania zamówienia potencjału technicznego i osobowego;
Załącznik nr 3 – Oświadczenie o wykonaniu w okresie 3 lat poprzedzających złożenie oferty minimum 1 diagnozy cyberbezpieczeństwa w ramach programu Cyfrowa Gmina oraz zrealizowania co najmniej 3 audytów bezpieczeństwa w jednostkach administracji publicznej o podobnym zakresie;
Załącznik nr 4 – Oświadczenie z danymi osoby posiadającej certyfikat o którym mowa w pkt IV;
Załącznik nr 5 - Oświadczenie o niepodleganiu wykluczeniu z udziału w postępowaniu;
Załącznik nr 6 - Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa;
Załącznik nr 7 - Klauzula informacyjna RODO