

Numer sprawy: IN.272.2.48.2022

Janowiec Wielkopolski, dnia 09.08.2022 r

Gmina Janowiec Wielkopolski

ul. Gnieźnieńska 3

88-430 Janowiec Wielkopolski

7-13-940, REGON 092351191

ZAPYTANIE OFERTOWE

na przeprowadzenie diagnozy cyberbezpieczeństwa oraz szkoleń w zakresie cyberbezpieczeństwa w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014—2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia – REACT-EU, Działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia.

I. ZAMAWIAJĄCY

Gmina Janowiec Wielkopolski

ul. Gnieźnieńska 3

88-430 Janowiec Wielkopolski

NIP: 562 171 39 40

Reprezentowana przez Burmistrza Janowca Wielkopolskiego.

II. TRYB POSTĘPOWANIA

1. Postępowanie o udzielenie zamówienia publicznego jest wyłączone z obowiązku stosowania ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz.U. 2021 poz. 1129 z późn.zm.) na podstawie art. 2 ust. 1 pkt 1).
2. Postępowanie o udzielenie zamówienia publicznego o wartości szacunkowej poniżej 20 000 zł netto prowadzone jest z zachowaniem zasad w sposób zapewniający przejrzystość oraz zachowanie równej, uczciwej konkurencji i równego traktowania wykonawcy.
3. Komunikacja w postępowaniu o udzielenie zamówienia, w tym składanie ofert, wymiana informacji oraz przekazywanie dokumentów lub oświadczeń między zamawiającym a wykonawcą, odbywa się przy użyciu środków komunikacji elektronicznej, za pośrednictwem platformy zakupowej Open Nexus.

III. OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest przeprowadzeniu diagnozy cyberbezpieczeństwa oraz szkoleń w zakresie cyberbezpieczeństwa w Urzędzie Miejskim w Janowcu Wielkopolskim w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014—2020, Oś V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia - REACT-EU, Działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, zgodnie z zakresem oraz formularzem stanowiącym załącznik do Regulaminu Konkursu Grantowego „Cyfrowa Gmina”.

2. PRZEPROWADZENIE DIAGNOZY CYBERBEZPIECZEŃSTWA:

- 2.1. Diagnoza musi zostać przeprowadzona w trybie stacjonarnym.
- 2.2. Diagnoza musi zostać przeprowadzona zgodnie z zakresem oraz formularzem stanowiącym załącznik nr 8 określonym w Regulaminie Konkursu Grantowego Cyfrowa Gmina, opublikowanego na stronie Centrum Projektów Polska Cyfrowa pod adresem <https://www.gov.pl/web/cppc/cyfrowa-gmina> oraz zgodnie z zapisami umowy o powierzenie grantu.

2.3. Diagnoza musi być przeprowadzona przez osobę posiadającą certyfikat uprawniający do przeprowadzenia audytu, o którym mowa 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.

2.4 Wvkaż certyfikatów uprawniających do przeprowadzania audvtu/diagnozy:

- Certified Internal Auditor (CIA)
- Certified Information System Auditor (CISA)
- 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
- 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
- Certified Information Security Manager (CISM)
- Certified in Risk and Information Systems Control (CRISC)
- Certified in the Governance of Enterprise IT (CGEIT)
- Certified Information Systems Security Professional (CISSP)
- Systems Security Certified Practitioner (SSCP)
- Certified Reliability Professional
- Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

2.5 W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany będzie do dokonania oceny zgodności funkcjonujących zasad i procedur dotyczących zarządzania bezpieczeństwem informacji, w tym przetwarzania danych osobowych, z obowiązującymi aktami prawnymi do przeprowadzenia diagnozy bezpieczeństwa informacji w zakresie ustawowych obszarów działalności podmiotu oraz opracowania dokumentacji - raportu zawierającego wnioski i rekomendacje.

2.6 Szczegółowy zakres przedmiotu zamówienia zawiera załącznik nr 8 do przedmiotowego Regulaminu „Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa”. Formularz ten stanowi załącznik nr 4 do niniejszego zapytania ofertowego. Wykonawca, którego oferta zostanie wybrana jako najkorzystniejsza, będzie zobligowany do podpisania wraz z umową o wykonanie diagnozy umowy o powierzeniu danych osobowych.

3.PRZEPROWADZENIE SZKOLENIA W ZAKRESIE CYBERBEZIECZEŃSTWA :

3.1 Szkolenie odbędzie się w siedzibie Zamawiającego, w trybie stacjonarnym. Zamawiający dopuszcza możliwość realizacji usługi za pomocą zdalnej komunikacji.

3.2. W szkoleniu będzie brało udział około 30 osób, w podziale na 2 grupy: I grupa -15 osób, II grupa 15 osób. Zamawiający dopuszcza rotacje w liczbie uczestników podczas każdego szkolenia.

3.3. Wymagane jest, aby każda z ww. grup miała szkolenie w innym terminie.

3.4. Szkolenia będą odbywać się w dni robocze, w godz. 8.00-15.00.

3.5. Szkolenia będą przeprowadzone w języku Polskim.



3.6. Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego dziennego harmonogramu prac, dostarczonego przez Wykonawcę Zamawiającemu nie później niż 7 dni przed rozpoczęciem szkolenia.

3.7. Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego szczegółowego zakresu merytorycznego szkolenia dostarczonego przez Wykonawcę.

3.8. W ramach organizacji szkoleń Wykonawca zapewni:

1) Materiały szkoleniowe, obejmujące szczegółowy zakres szkolenia, harmonogram dzienny szkolenia oraz materiały merytoryczne (np. skrypty, podręczniki, zeszyty informacyjne, broszury) w formie papierowej, zawierające szczegółowe informacje, które będą omawiane podczas szkolenia. Ponadto, uczestnicy otrzymają materiały pisarskie, w tym zeszyty, długopisy, ołówki itp. Materiały szkoleniowe przekazywane są nieodpłatnie Uczestnikom na własność. 2 egzemplarze materiałów szkoleniowych zostaną przekazane Zamawiającemu w celach archiwalnych.

2) Wydanie Uczestnikom szkolenia zaświadczeń o ukończeniu danego szkolenia.

3) Kadre trenerską posiadającą wiedzę i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkoleń.

4) Prowadzenie dokumentacji wszystkich szkoleń w jednaki sposób. Na dokumentację szkolenia składają się:

a) Lista obecności Uczestników szkolenia;

b) Lista odbioru zaświadczeń o ukończeniu szkolenia.

c) Potwierdzenie przez Uczestników odbioru materiałów szkoleniowych.

d) Przeprowadzenie ankiet satysfakcji po każdym szkoleniu.

e) Sporządzony przez kadre trenerską dziennik zajęć, zawierający szczegółowe informacje na temat przebiegu oraz zakresu merytorycznego szkolenia, podpisany po zakończeniu szkolenia przez prowadzącego szkolenie.

Ramowy zakres szkolenia:

1. Główne założenia i wymagania prawne cyberbezpieczeństwa w pracy urzędnika.

2. Polityka bezpieczeństwa w organizacji.

3. Definicja incydentu bezpieczeństwa i zasady postępowania z incydem.

4. Rodzaje ataków: ataki socjotechniczne, ataki komputerowe, ataki przez sieci bezprzewodowe, ataki przez pocztę e-mail (fałszywe e-maile), ataki przez strony WWW, ataki przez telefon, phishing, spoofing, spam.

5. Bezpieczeństwo fizyczne - urządzenia, dokumenty, „czyste biurko”.

6. Prawidłowe korzystanie z oprogramowania antywirusowego.

7. Zasady aktualizacji programów i aplikacji.

8. Szyfrowanie dokumentów i poczty elektronicznej.

9. Polityka haseł, zarządzanie dostępem i tożsamością.

IV. OZNACZENIE PRZEDMIOTU ZAMÓWIENIA

Oznaczenie przedmiotu zamówienia wg. Wspólnego Słownika Zamówień (CPV):

- usługi audytu- 79212000-3;

- szkolenia - usługi szkoleniowe -80500000-9.

- usługi audytu komputerowego i testowania komputerów-72800000-8

- usługi audytu komputerowego-72810000-1

V. TERMIN WYKONANIA ZAMÓWIENIA:

1. Przeprowadzenie szkolenia dla urzędników w zakresie cyberbezpieczeństwa – usługę będzie przeprowadzona w terminie do 30.11.2022 r.
2. Przeprowadzenie diagnozy cyberbezpieczeństwa zgodnie z założeniami projektu Cyfrowa Gmina- usługę będzie przeprowadzona w terminie do 30.09.2022 r.

VI. KRYTERIA WYBORU NAJKORZYSTNIEJSZEJ OFERTY

1. Kryterium oceny ofert - Cena 100%.
2. Wykonawca określi cenę oferty, która stanowić będzie wynagrodzenie ryczałtowe za realizację całego przedmiotu zamówienia, podając ją w zapisie liczbowym i słownie z dokładnością do grosza (do dwóch miejsc po przecinku).
3. Cena oferty musi zawierać wszystkie koszty niezbędne do zrealizowania przedmiotu zamówienia. Wykonawca musi uwzględnić w cenie oferty wszelkie koszty niezbędne dla prawidłowego i pełnego wykonania zamówienia ujęte w zał. nr 1 do Zapytania oraz wszelkie opłaty i podatki wynikające z obowiązujących przepisów.
4. Za najkorzystniejszą zostanie uznana oferta Wykonawcy, który zaoferuje najniższą cenę całkowitą za wykonanie przedmiotu zamówienia.

VII. OFERTA MUSI ZAWIERAĆ NASTĘPUJĄCE DOKUMENTY

- 1) Formularz ofertowy - załącznik nr 1 do zapytania.

Formularz ofertowy oraz pozostałe dokumenty muszą zostać podpisane podpisem własnoręcznym i zeskanowane, następnie przesłane przez platformę zakupową. Zamawiający dopuszcza zastosowanie podpisu elektronicznego kwalifikowanego, podpisu zaufanego lub podpisu osobistego zamiast podpisu własnoręcznego.

Jeżeli w imieniu wykonawcy działa osoba, której umocowanie do jego reprezentowania nie wynika z odpisu lub informacji z Krajowego Rejestru Sądowego, Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub innego właściwego rejestru, zamawiający żąda od wykonawcy pełnomocnictwa lub innego dokumentu potwierdzającego umocowanie do reprezentowania wykonawcy.

- 2) Oświadczenie o posiadanych doświadczeniach- załącznik nr 3 do zapytania.
- 3) Oświadczenie z danymi osoby posiadającej wymagane uprawnienia- załącznik nr 4 do zapytania.
- 4) Oświadczenie o niepodleganiu wykluczenia z postępowania na podstawie ustawy z 13.4.2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego- załącznik nr 6 do zapytania.

VIII. SPOSÓB ZŁOŻENIA OFERTY I OTWARCIE OFERT

1. Wykonawca może złożyć jedną ofertę.
2. Ofertę należy złożyć wyłącznie elektronicznie za pomocą Platformy Zakupowej Gminy Janowiec Wielkopolski w terminie do dnia **16.08.2021 r. do godziny 10.00**, na załączonym wzorze formularza ofertowego.
3. Otwarcie ofert nastąpi w dniu **16.08.2021 r. o godz. 10.10**.
4. Ofertę pod rygorem nieważności składa się w formie pisemnej w języku polskim.
5. Cena oferty musi obejmować wszelkie koszty oraz być podana w kwotach netto i brutto podanych do dwóch miejsc po przecinku, wyrażonej cyfrowo w złotych polskich z wyodrębnieniem należnego podatku VAT - jeżeli występuje.



5. Nie dopuszcza się wariantowości oferty — oferta powinna zawierać wszystkie wskazane przez Zamawiającego elementy.

IX. WARUNKI UDZIAŁU W POSTĘPOWANIU:

- Wykonawca musi wykazać, że w okresie ostatniego 1 roku przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wykonał (zakończył) co najmniej 1 diagnozę cyberbezpieczeństwa w ramach konkursu „Cyfrowa Gmina”. Wykonawca złoży w tym zakresie oświadczenie (załącznik nr 3) będące załącznikiem do oferty wraz z dokumentem potwierdzającym należyte wykonanie.

Dokumentami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego usługa została wykonana a jeżeli wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tego dokumentu – oświadczenie Wykonawcy. Zamawiający zastrzega sobie prawo do weryfikacji oświadczenia pod kątem zgodności ze stanem faktycznym.

- Wykonawca musi dysponować osobą posiadającą uprawnienia, o których mowa w Rozdziale III ust.2 pkt. 2.2 niniejszego zapytania ofertowego. Wykonawca złoży w tym zakresie oświadczenie (załącznik nr 2) będące załącznikiem do oferty

- Wykonawca nie może podlegać wykluczenia z postępowania na podstawie ustawy z 13.4.2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz.U. z 2022 poz. 835).

W tym zakresie Wykonawca składa wraz z ofertą oświadczenie- załącznik nr 6 do zapytania ofertowego.

X. OSOBAMI UPRAWNIONYMI DO KONTAKTÓW Z RAMIENIA ZAMAWIAJĄCEGO SĄ

Dominika Raczyńska i Joanna Lubawa-Fura – Urząd Miejski w Janowcu Wielkopolskim,

e-mail: d.raczynska@um-janowiecwlkp.pl

XI. DODATKOWE INFORMACJE

1. Zamawiający zastrzega sobie możliwość negocjacji zaoferowanej ceny, w przypadku, gdy założone w projekcie środki okażą się niewystarczające.
2. Oferta może zostać odrzucona, jeśli zawiera rażąco niską cenę w stosunku do przedmiotu zamówienia.
3. Ewentualna zmiana terminu i/lub miejsca realizacji możliwa jest tylko za zgodą zamawiającego; w szczególności w związku z ewentualnymi zmianami w realizacji projektu.
4. Zamawiający zastrzega sobie możliwość wprowadzania modyfikacji do zapytania. Informację o dokonanej modyfikacji przekaże również drogą mailową wszystkim oferentom, którzy złożą ofertę przed jej dokonaniem.
5. Zamawiający - w celu zachowania zasady uczciwej konkurencji i równego traktowania - nie stosuje ograniczeń personalnych ani terytorialnych w stosunku do oferentów.

Nabór prowadzony będzie z zachowaniem zasady równości szans i niedyskryminacji –bez względu na płeć, wiek, niepełnosprawność, rasę lub pochodzenie etniczne, wyznawaną religię lub światopogląd czy orientację seksualną.

6. Zamawiający zastrzega sobie prawo zakończenia postępowania w sprawie wyboru wykonawcy zadania, bez wyboru żadnej z ofert – bez podania przyczyny.

XII. TERMIN ZWIĄZANIA Z OFERTĄ

Termin związania ofertą wynosi 30 dni

XIII. INFORMACJE KOŃCOWE

1. Niniejsze postępowanie prowadzone jest zgodnie z przepisami ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz.U. 2020 poz. 1740 z późn. zm.).
2. Zgodnie z art. 701 § 3 ustawy Kodeks cywilny Zamawiający zastrzega sobie możliwość zmiany lub odwołania warunków niniejszego zapytania do upływu terminu składania ofert.
3. Zamawiający zastrzega, że może podjąć negocjacje cenowe z Wykonawcą biorącym udział w przedmiotowym Zapytaniu ofertowym.
4. Zamawiający zgodnie z art. 703 § 2 ustawy Kodeks cywilny zobowiązuje się niezwłocznie powiadomić na piśmie uczestników postępowania o jego wyniku albo o zamknięciu postępowania bez dokonania wyboru.
5. Zamówienie jest współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa, Oś V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia - REACT-EU, Działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia.

BURMISTRZ

Leszek Grzeczka

ZAŁĄCZNIKI:

- Załącznik nr 1 –Formularz ofertowy;
- Załącznik nr 2- Oświadczenie Wykonawcy-osoba z certyfikatem;
- Załącznik nr 3- Oświadczenie-doświadczenie;
- Załącznik nr 4- Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa;
- Załącznik nr 5-Projekt umowy;
- Załącznik nr 6-Oświadczenie Wykonawcy dot. wykluczenia;