GMINA ORCHOWO
ul. Kościuszki 6, 62 – 436 Orchowo
woj. wielkopolskie
tel./fax 063/ 2684090
NIP: 6671735111, REGON: 311019378

Orchowo, dnia 26.08.2022 r.

ZW.271.5.2022

ZAPYTANIE OFERTOWE
na wykonanie **DIAGNOZY CYBERBEZPIECZEŃSTWA**
w ramach projektu grantowego pn. „Cyfrowa Gmina" nr POPC.05.01.00-00-0001/21-00 realizowanego w ramach Programu Operacyjny 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

I. ZAMAWIAJĄCY

Gmina Orchowo
ul. Kościuszki 6
62-436 Orchowo
Tel. 63 2684090
NIP 667-173-51-11
REGON 311019378
www.orchowo.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 (Dz. U. 2021 poz. 1129 z późn. zm.) na podstawie art. 2 ust. 1 pkt
2. Postępowanie o udzielenie zamówienia publicznego o wartości szacunkowej poniżej 50 000 zł netto prowadzone jest w oparciu o rozeznanie rynku zgodnie z rozdziałem 6.5.1 Wytycznych w zakresie kwalifikowalności wydatków w ramach Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności na lata 2014-2020 oraz na podstawie Regulaminu udzielania zamówień publicznych o wartości poniżej kwoty wskazanej w art. 2 ust. 1 pkt. 1 ustawy Prawo Zamówień Publicznych przyjętym Zarządzeniem Wójta Gminy Orchowo.

III. KODY CPV

72800000-8 Usługi audytu komputerowego i testowania komputerów
72810000-1 Usługi audytu komputerowego
79212000-3 Usługi audytu

IV. OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest wykonanie **diagnozy cyberbezpieczeństwa** w ramach projektu grantowego pn. „Cyfrowa Gmina" nr POPC.05.01.00-00-0001/21-00 realizowanego w ramach Programu Operacyjny 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.

1. Audyt bezpieczeństwa danych w systemach informatycznych oraz sieci ICT:
1.1 Analiza wszystkich zabezpieczeń przed utratą i kradzieżą danych
1.2 Analiza kontroli dostępu do systemów informatycznych w tym dostępu przez usługi i narzędzia

zdalne
1.3 Analiza zabezpieczeń przy pracy zdalnej
1.5 Analiza i ocena technicznej infrastruktury w systemach ICT, schematu sieci a także technicznych zabezpieczeń sieci.
1.6 Analiza i ocena zabezpieczeń dostępu do sieci publicznej
1.7 Analiza i ocena zabezpieczeń wewnętrznej sieci ICT
1.8 Ocena sposobu identyfikowania i logowania użytkowników
1.9 Analiza i ocena systemów backupów i archiwizacji danych w tym testy odtworzeniowe.
1.10 Analiza i ocena ciągłości pracy systemów i sieci ICT
1.11 Testy penetracyjne systemów informatycznych i całej infrastruktury ICT
1.12 Sprawdzenie zabezpieczeń komputerów przed atakami phishingowymi
1.13 Badanie podatności usług sieciowych
1.14 Badanie podatności aplikacji serwera pocztowego email i aplikacji webowej zgodnie z OWASP.
1.15 Weryfikacja systemu uwierzytelniania użytkowników i administratorów
1.16 Weryfikacja systemu uwierzytelniania użytkowników i administratorów do systemu operacyjnego i kontrolera domeny
1.17 Sprawdzenie sposobów i systemów szyfrowania m.in. protokoły szyfrowania, szyfrowanie danych END-to-END w poczcie email itp.
1.18 Sprawdzenie i ocena szyfrowania danych przechowywanych poza Urzędem m.in. serwisy pocztowe email, serwisy WEB itp.
1.19 Sprawdzenie systemów ochrony poczty email i usług WEB pod kątem ataków phishingowych
1.20 Analiza i ocena sposobu zbierania logów, zakresu i retencji logów
1.21 Identyfikacja pojedynczych punktów awarii

2. Audyt ochrony danych zgodnie z przepisami RODO, UODO, KRI, KSC
2.1 Analiza zgodności dokumentacji ochrony danych osobowych
2.2 Analiza upoważnień do przetwarzania danych osobowych
2.3 Analiza umów powierzenia przetwarzania danych osobowych
2.4 Analiza umów i porozumień dotyczących przekazywania danych osobowych
2.5 Analiza rejestru czynności przetwarzania oraz rejestru kategorii czynności przetwarzania
2.6 Ocena procesu zarządzania incydentami i reagowania na incydenty. Analiza informacji lub raportów dotyczących, incydentów naruszenia bezpieczeństwa danych
2.7 Analiza konieczności dokonania oceny skutków dla planowanych sposobów przetwarzania danych
2.8 Rozpoznanie roli i funkcji IODO
2.9 Rozpoznanie wszystkich systemów przetwarzających dane i ich konfigurację
2.10 Rozpoznanie wszystkich przetwarzanych zbiorów danych
2.11 Kontrola zabezpieczeń zbiorów tradycyjnych
2.12 Kontrola zabezpieczeń zbiorów archiwalnych
2.13 Kontrola systemu monitoringu
2.14 Kontrola systemu alarmowego
2.15 Weryfikacja kontroli nad przepływem danych osobowych
2.16 Weryfikacja poufności, dostępności i udostępniania danych osobowych
2.17 Analiza i ocena zagrożeń z identyfikacją słabych stron związanych z przetwarzaniem danych
2.18 Weryfikacja dostępu osób nieupoważnionych do miejsc, gdzie przetwarzane są dane
2.19 Analiza i ocena procedur zarządzania systemami teleinformatycznymi
2.20 Analiza i ocena zaangażowania Najwyższego Kierownictwa w proces ciągłego doskonalenia systemu bezpieczeństwa informacji

2.21 Analiza i ocena ochrony ICT przed oprogramowaniem szkodliwym, w tym weryfikacja zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania
2.22 Analiza i ocena procedur historii zmian w dokumentach, systemach informatycznych itp.
2.23 Analiza i ocena procedur zarządzania i zabezpieczania nośników przechowujących dane
2.24 Analiza i ocena zasad odpowiedzialności użytkowników
2.25 Analiza i ocena zasad zarządzania hasłami
2.26 Analiza i ocena zabezpieczeń kryptograficznych
2.27 Analiza i ocena zabezpieczeń komputerów przenośnych w tym praca zdalna.
2.28 Analiza stopnia zabezpieczenia stacji roboczych i nośników danych w szczególności tych, na których przetwarzane są dane osobowe
2.29 Analiza i ocena niszczenia niepotrzebnych nośników oraz danych
2.30 Analiza i ocena stron webowych pod kątem zgodności standardu min. WCAG 2.1

3. Opracowanie raportu zawierającego ocenę stosowanych zabezpieczeń, analizę stanu bezpieczeństwa, wnioski, zalecenia i rekomendację dotyczące zakresu, metodyki i organizacji zabezpieczeń

4.
4.1 Diagnoza cyberbezpieczeństwa (audyt) musi zostać przeprowadzona zgodnie z Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560 z późn. zm.) oraz Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tj. Dz.U. 2017 poz. 2247 ze zm.) zwane dalej Rozporządzeniem KRI

4.2
Diagnoza musi zostać wykonana zgodnie z formularzem zamieszczonym w dokumentacji konkursowej projektu Cyfrowa Gmina dostępnym na stronach Centrum Projektów Polska Cyfrowa [https://www.gov.pl/web/cppc/cyfrowa-gmina] - Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa - załącznik nr 8.

4.3 Audyt musi zostać przeprowadzony 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 w/w rozporządzeniu:
a) Certified Internal Auditor (CIA)
b) Certified Information System Auditor (CISA)
c) 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
d) 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
e) Certified Information Security Manager (CISM)
f) Certified in Risk and Information Systems Control (CRISC)
g) Certified in the Governance of Enterprise IT (CGEIT)
h) Certified Information Systems Security Professional (CISSP)

i) Systems Security Certified Practitioner (SSCP)
j) Certified Reliability Professional
k) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert

Wynikiem audytu jest:
1. pełny raport z przeprowadzonego audytu
2. rekomendacje dotyczące technicznych zabezpieczeń danych i informacji

V. ZAKRES OBOWIĄZKÓW WYKONAWCY

Wykonawca zobowiązany jest do kompleksowej realizacji zamówienia tzn. wykonania diagnozy cyberbezpieczeństwa, wypełnienie i podpisanie wymaganych dokumentów zgodnie Z Regulaminem Konkursu Grantowego Cyfrowa Gmina i zapisami umowy o powierzenie grantu oraz ich dostarczenie w wersji elektronicznej i papierowej do siedziby Zamawiającego (po jednym egzemplarzu).
W ramach zamówienia Wykonawca zobowiązany jest do przeprowadzenia diagnozy cyberbezpieczeństwa w siedzibie Zamawiającego. Zamawiający nie dopuszcza możliwości realizacji usługi za pomocą środków zdalnej komunikacji. Audyt powinien być wykonany na miejscu w siedzibie Urzędu Gminy Orchowo, ul. Kościuszki 6, 62-436 Orchowo.
Wykonawca zobowiązany jest do pokrycia wszystkich kosztów związanych z wykonaniem przedmiotu zamówienia, w tym koszty ewentualnego zakwaterowania, dojazdu, wyżywienia, wydruku i skanu dokumentów.
Wykonawca zobowiązany jest do współpracy i konsultacji z Zamawiającym oraz do wprowadzania poprawek w sporządzanej przez siebie dokumentacji na każdym etapie realizacji zamówienia, aż do zaakceptowania dokumentów wystawionych przez Wykonawcę przez Grantodawcę Konkursu Cyfrowa Gmina.

VI. TERMIN WYKONANIA ZAMÓWIENIA

30 dni od podpisania umowy.

VII. WARUNKI UDZIAŁU W POSTĘPOWANIU

O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy:
1. posiadają niezbędną wiedzę i doświadczenie oraz dysponują potencjałem technicznym i osobami zdolnymi do wykonania zamówienia (Wykonawca złożył w tym zakresie oświadczenie będący załącznikiem do oferty),
2. posiadają doświadczenie w wykonywaniu audytów - Wykonawca wykaże, że wykonał minimum 1 audyt/diagnozę w ramach konkursu „Cyfrowa Gmina" lub zrealizował co najmniej 2 audyty - w jednostkach administracji publicznej o podobnym zakresie w ostatnich 3 latach przed złożeniem oferty (Wykonawca złoży w tym zakresie oświadczenie będące załącznikiem do oferty wraz z dokumentami potwierdzającymi wykonanie),
3. posiadają uprawnienia do wykonywania określonej działalności lub czynności jeśli ustawy nakładają obowiązek posiadania takich uprawnień – w tym certyfikaty wymienione w pkt. IV. 4.3. Wykonawca złoży kopie wymaganych certyfikatów.
4. znajdują się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia.

VIII. WYMAGANE DOKUMENTY DO ZŁOŻENIA WRAZ Z OFERTĄ

1. Formularz ofertowy – załącznik nr 1 do zapytania,
2. Oświadczenie, że wykonawca spełnia warunki udziału w postępowaniu określone w punkcie VII - załącznik nr 2 do zapytania,
3. Oświadczenie wykonawcy o posiadanym doświadczeniu – załącznik nr 3 do zapytania wraz z kopią certyfikatów uprawniających do przeprowadzenia audytu,
4. Dane osoby, która będzie wykonywała diagnozę wraz z dokumentem potwierdzającym posiadanie przez nią certyfikatu uprawniającego do przeprowadzenia 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.

IX. OPIS SPOSOBU PRZYGOTOWANIA OFERTY

1. Wykonawca może złożyć jedną ofertę.
2. Wykonawca składa ofertę na formularzu oferty załączonym do niniejszego zapytania. Ofertę pod rygorem nieważności składa się w formie pisemnej w języku polskim. Do oferty należy dołączyć komplet wymaganych dokumentów zarządanych w pkt. VIII niniejszego zapytania.
3. Cena wynikająca z oferty winna obejmować wszelkie koszty oraz być podana w kwotach netto i brutto podanych do dwóch miejsc po przecinku, wyrażonej cyfrowo i słownie w złotych polskich z wyodrębnieniem należnego podatku VAT - jeżeli występuje.
4. Nie dopuszcza się wariantowości oferty - oferta powinna zawierać wszystkie wskazane przez Zamawiającego elementy.

X. MIEJSCE I TERMIN SKLADANIA OFERT

Ofertę należy złożyć **do dnia 06.09.2022 r. do godz. 10.00** w jednej z następujących form:

- osobiście lub przesyłką pocztową do Sekretariatu (I piętro) w siedzibie Zamawiającego (Urząd Gminy Orchowo, ul. Kościuszki 6, 62-436 Orchowo czynny jest od poniedziałku do piątku w godz. 07:30 - 15:30).

O zachowaniu terminu decyduje data wpływu oferty do siedziby Zamawiającego.

Oferty złożone po wyznaczonym terminie nie będą rozpatrywane.

Liczy się data faktycznego wpływu oferty do siedziby Zamawiającego a nie data stempla pocztowego dowodu nadania.
Otwarcie ofert nastąpi 06.09.2022 r. o godz. 10.15 na Sali Narad UG Orchowo.

XI. OCENA OFERT

1. Jedynym kryterium oceny ofert (100%) będzie **cena całkowita** za wykonanie przedmiotu zamówienia opisanego w niniejszym zapytaniu wynikająca z oferty cenowej sporządzonej przez Wykonawcę zgodnie z formularzem ofertowym stanowiącym załącznik nr 1 do niniejszego zapytania.

W kryterium cena ocena ofert zostanie przeprowadzona wg formuły:

$$\text{Otrzymane punkty} = \frac{\text{Cena najniższa spośród złożonych ofert}}{\text{Cena badanej oferty}} \times 100$$

2. Zamówienie zostanie udzielone Wykonawcy, który spełnia wszystkie wymienione wymagania oraz przedstawi najkorzystniejszą ofertę cenową tj. uzyskał największą liczbę punktów.
3. W przypadku gdy w postępowaniu zostaną złożone dwie lub więcej ofert z jednakową ceną, zamawiający zastrzega sobie prawo do prowadzenia negocjacji z tymi Wykonawcami lub poproszenia o złożenie ofert ponownych.
4. Zamawiający nie będzie oceniał oferty:
    a. jeżeli jej treści nie będzie odpowiadać treści zapytania ofertowego,
    b. zostanie złożona po terminie składania ofert,
    c. nie będzie zabierała wszystkich wymaganych załączników,
    d. będzie nieważna na podstawie odrębnych przepisów.

XII. INFORMACJE DOTYCZĄCE WYBORU NAJKORZYSTNIEJSZEJ OFERTY

Informacja o wyborze oferty zostanie podana na stronie BIP Orchowo w zakładce „Zamówienia publiczne" – „Zamówienia publiczne do kwoty 130.000 złotych".

XIII. TERMIN ZWIĄZANIA OFERTĄ

Termin związania ofertą wynosi 30 dni.

XIV. DODATKOWE INFORMACJE

1. Przy wyborze oferty zamawiający kierować się będzie jedynym kryterium „cena". Cena za wykonanie zamówienia obejmuje wszystkie koszty niezbędne do całkowitego i efektywnego wykonania zamówienia.
2. Zamawiający zastrzega sobie prawo do:
    a. zamknięcia niniejszego postępowania bez wyboru jakiejkolwiek oferty i bez podania przyczyny o czym poinformuje niezwłocznie oferentów.
    b. wezwania wykonawców do wyjaśnień lub uzupełnienia dotyczących informacji zawartych w ofercie.
    c. zmiany treści zapytania ofertowego przed upływem terminu składania ofert.
3. Dodatkowych informacji dotyczących zapytania ofertowego udziela: Paweł Błaszczyk, tel. 63 26 84 090 wew. 25,
   e-mail: adm@orchowo.pl

XV. ZAŁĄCZNIKI

1) Formularz ofertowy,
2) Wzór oświadczenia dotyczącego spełniania warunków udziału w postępowaniu przez Wykonawcę,
3) Wzór oświadczenia o posiadanym doświadczeniu,
4) Wzór oświadczenia z danymi osoby posiadającej certyfikat, o którym mowa w pkt. IV.

wz. Wójta
Ewelina Gumienna
Zastępca Wójta