GMINA ŁUBNICE
ul. gen. Sikorskiego 102
98-432 Łubnice
tel. 62 78 47 027 fax 62 78 47 015
NIP 997-01-32-801 Regon 250855506

Łubnice, dnia 15.07.2025r.

RI.271.2.32.2025.KM

Zapytanie ofertowe

I. Zamawiający

Gmina Łubnice, ul. gen. Sikorskiego 102, 98-432 Łubnice NIP: 9970132801 REGON: 250855506

II. Tryb udzielenia zamówienia

Postępowanie prowadzone jest bez zastosowania ustawy z dnia 11.09.2019r. Prawo zamówień publicznych – wartość zamówienia nie przekracza kwoty 130 000,00 zł netto. Postępowanie prowadzi się w oparciu o Regulamin udzielania zamówień publicznych, których wartość nie przekracza kwoty 130 000,00 zł netto, stanowiący załącznik do zarządzenia nr 0050.45.2025 Wójta Gminy Łubnice z dnia 4 lipca 2025r. w sprawie wprowadzenia w Urzędzie Gminy Łubnice regulaminu udzielania zamówień publicznych, których wartość nie przekracza 130 000,00 złotych netto.

III. Przedmiot zamówienia:

Przedmiotem zamówienia jest przeprowadzenie dedykowanego szkolenia dla pracowników Urzędu Gminy Łubnice z zakresu podstaw cyberbezpieczeństwa i zagrożeń z nim związanych.

IV. Szczegółowy opis przedmiotu zamówienia:

1. Przeprowadzenie w okresie do dnia 31.10.2025r. dedykowanego szkolenia dla 30 pracowników Urzędu Gminy Łubnice z zakresu podstaw cyberbezpieczeństwa i zagrożeń z nim związanych w ramach zadania inwestycyjnego pn. Przeprowadzenie szkolenia dla pracowników w ramach projektu grantowego „Cyberbezpieczny Samorząd". Szkolenie przeznaczone będzie dla pracowników Urzędu Gminy Łubnice, którzy wykonując zadania służbowe posługują się komputerem lub telefonem i mają dostęp do Internetu. Szkolenie powinno kształtować świadomość pracowników w zakresie różnych wariantów najpopularniejszych ataków, jakie są stosowane, uczyć jak się przed tymi atakami ustrzec oraz wprowadzać dobre praktyki dotyczące dbania o bezpieczeństwo.
2. **Szkolenie powinno min. obejmować następujące zagadnienia:**
    1. Znaczenie Cyberbezpieczeństwa i pojęcia z nim związane.
    2. Aktualne zagrożenia w cyberprzestrzeni.
    3. Dlaczego JST są celem ataków?
    4. Tworzenie silnych haseł i zarządzanie nimi.
    5. Znaczenie uwierzytelniania wieloskładnikowego.
    6. Aktualizacja oprogramowania i systemów.
    7. Używanie nośników zewnętrznych.
    8. Phishing i ataki typu spear-phishing.
    9. Malware, ransomware i wirusy.
    10. Ataki Dos/DDoS.
    11. Socjotechnika i media społecznościowe.
    12. Jak rozpoznać podejrzane wiadomości?

13. Zabezpieczanie skrzynek pocztowych.
14. Znaczenie szyfrowania i podpisu cyfrowego w komunikacji.
15. Bezpieczne przeglądanie stron internetowych.
16. Bezpieczne korzystanie z sieci WiFi.
17. Bezpieczne korzystanie z mediów społecznościowych.
18. Używanie VPN w miejscach publicznych.
19. Kopia zapasowa danych i jego znaczenie.
20. Zabezpieczanie urządzeń mobilnych.
21. Fizyczne zabezpieczenie sprzętu.
22. Jak postępować w przypadku podejrzenia naruszenia bezpieczeństwa?
23. Co to są polityki i procedury bezpieczeństwa?
24. Komunikacja wewnętrzna i zewnętrzna.
25. RODO (GDPR) i ochrona danych osobowych.
26. Dane wrażliwe i niewrażliwe.
27. Krajowe przepisy dotyczące Cyberbezpieczeństwa.
28. Obowiązki pracowników urzędu w zakresie ochrony danych.
29. Symulacja ataków phishingowych.
30. Praktyczne ćwiczenia z zakresu tworzenia haseł.
31. Analiza przypadków naruszeń bezpieczeństwa.
32. Pokazy na żywo dotyczące działania wirusów, ransomware, itp.
33. Sposób myślenia przestępców – przykład i warsztat
34. Najważniejsze zasady bezpieczeństwa w pracy urzędnika.
35. Znaczenie ciągłego doskonalenia w zakresie Cyberbezpieczeństwa.
36. Podstawy prawne krajowego systemu cyberbezpieczeństwa, obowiązki wynikające z ustawy, procedury zgłaszania incydentów.

3. Pominięcie przez Zamawiającego jakiegokolwiek zagadnienia z ww. zakresu nie zwalnia Wykonawcy z prawidłowego wykonania szkoleń zgodnie z projektem „Cyberbezpieczny Samorząd" w ramach działania 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa.
4. Miejsce wykonania przedmiotu umowy: Urząd Gminy Łubnice, ul. gen. Sikorskiego 102, 98-432 Łubnice.
5. Zamówienie będzie finansowane ze środków otrzymanych z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa konkurs grantowy w ramach projektu grantowego „Cyberbezpieczny Samorząd", wobec czego wykonawca będzie zobligowany do współpracy z zamawiającym w zakresie prawidłowego przeprowadzenia i rozliczenia przedmiotu umowy.

V. Termin realizacji zamówienia: od dnia podpisania umowy do dnia 31.10.2025r.

VI. Kryterium oceny ofert: Cena brutto – 100%.

VII. Termin płatności: 14 dni od dnia dostarczenia Zamawiającemu prawidłowo wystawionej faktury

VIII. Istotne warunki zamówienia (w tym termin gwarancji i rękojmi):

1. Warunki udziału w postępowaniu:

1) przedstawienie oferty handlowej na przeprowadzenia kompleksowej usługi szkolenia zgodnie z opisem przedmiotu zamówienia
2) wykazanie, że posiada lub dysponuje osobą skierowaną do realizacji zamówienia posiadającą przynajmniej jeden certyfikat wykazany w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018r. w sprawie wykazu certyfikatów uprawniających do przeprowadzania audytu w rozumieniu art. 15 ustawy z dnia 5 lipca 2018r. o krajowym systemie cyberbezpieczeństwa (CISSP)
   Akceptowane przez Zamawiającego certyfikaty, to w szczególności: Audytor wewnętrzny i zewnętrzny normy PN-ISO/IEC 27001, CISA, CIA oraz równoważne poświadczenia/certyfikaty z zakresu cyberbezpieczeństwa. Listy referencyjne wraz z opisami wcześniejszych projektów.
3) posiadanie stosownej wiedzy oraz minimum 2-letnie doświadczenie w przygotowaniu i przeprowadzeniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń, poświadczone odpowiednimi referencjami. Zamawiający wymaga udokumentowania doświadczenia w przeprowadzenia minimum 10 szkoleń w okresie 2 lat poprzedzających datę ogłoszenia niniejszego zapytania ofertowego.

IX. Forma złożenia oferty:

Ofertę należy przesłać lub złożyć **w terminie do dnia 31.07.2025r. do godziny 12:00** na formularzu ofertowym będącym załącznikiem do niniejszego zapytania ofertowego w Urzędzie Gminy Łubnice, ul. gen. Sikorskiego 102, 98-432 Łubnice lub drogą elektroniczną na adres: uglubnice@uglubnice.com.pl

X. Osoby uprawnione do porozumiewania się z Wykonawcami:

Anita Borgul – Stanowisko ds. inwestycji i zamówień publicznych e-mail: przetargi@uglubnice.com.pl tel: 627847028

XI. Informacja o sposobie powiadomienia o wynikach prowadzonego postępowania.

1. Niezwłocznie po wyborze najkorzystniejszej oferty Zamawiający zawiadomi Wykonawców, którzy złożyli ofertę o wyborze najkorzystniejszej oferty drogą elektroniczną na adres mailowy podany w ofercie.
2. O zakończeniu postępowania bez wyboru oferty Zamawiający powiadomi niezwłocznie Wykonawców, którzy złożyli ofertę drogą elektroniczną na adres mailowy podany w ofercie.

XII. Zamawiający zastrzega sobie prawo do odwołania niniejszego ogłoszenia i jego warunków oraz do unieważnienia postępowania.

XIII. Informacje dodatkowe:

XIV. Wykaz oświadczeń i dokumentów, jakie mają dostarczyć Wykonawcy w celu potwierdzenia spełniania warunków udziału w postępowaniu:

1. Dokument potwierdzający wypełnienie obowiązku informacyjnego w zakresie przetwarzania danych osobowych
2. Oświadczenie wymagane od wykonawcy w zakresie wypełnienia obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO
3. Formularz ofertowy

4. Poświadczenie (referencje) dotyczące potwierdzenia 2-letniego okresu doświadczenia w przygotowaniu i przeprowadzeniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń.
5. Wykazanie, że posiada lub dysponuje osobą skierowaną do realizacji zamówienia posiadającą co najmniej jeden certyfikat wykazany w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenie audytu w rozumieniu art. 15 ustawy z dnia 5 lipca 2018r. o krajowym systemie cyberbezpieczeństwa (CISSP). Należy przedstawić wykaz osób skierowanych do realizacji zamówienia wraz z wykazaniem ich uprawnień.
6. Oświadczenie o zapoznaniu się z Regulaminem konkursu „Cyberbezpieczny samorząd"
7. Program szkolenia

WÓJT
Tomasz Pawlik
.....

(podpis Zamawiającego lub osoby upoważnionej do działania w jego imieniu)

Do zapytania dołączono:

1. Dokument potwierdzający wypełnienie obowiązku informacyjnego w zakresie przetwarzania danych osobowych
2. Oświadczenie wymagane od wykonawcy w zakresie wypełnienia obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO
3. Projekt umowy
4. Formularz ofertowy
5. Umowa powierzenia danych