Realizacja projektu w ramach Umowy o powierzenie grantu o numerze 3413/1/2021 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT - EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina" o numerze POPC.05.01.00-00-0001/21-00.

Ozimek, dnia 24 lipca 2023 roku

Zapytanie ofertowe S.271.16.2023.BD

na przeprowadzenie szkolenia pracowników Urzędu Gminy i Miasta w Ozimku i jednostek organizacyjnych z zakresu cyberbezpieczeństwa realizowane w ramach projektu „Cyfrowa Gmina”

I. **Zamawiający:** Gmina Ozimek, ul. ks. Jana Dzierżona 4B, 46-040 Ozimek (991-03-25-175), zaprasza do złożenia oferty w postępowaniu wyłączonym z zakresu przedmiotowego ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych.

II. Opis przedmiotu zamówienia.

Przeprowadzenie szkolenia wszystkich pracowników Urzędu Gminy i Miasta w Ozimku i jednostek organizacyjnych z zakresu cyberbezpieczeństwa.

III. Czas szkolenia :

Minimalny wymiar czasu – 4 godziny zegarowe.

Liczba uczestników: 20 osób

IV. Zakres szkolenia :

Przedmiotem zamówienia jest przeprowadzenie **szkolenia w zakresie cyberbezpieczeństwa,** dotyczącego praktycznego stosowania mechanizmów bezpieczeństwa korespondencji i zabezpieczania danych, w ramach projektu pn. „Cyfrowa Gmina” realizowanego w ramach Programu Operacyjny Polska Cyfrowa na lata2014-2020, 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.
Szkolenie powinno składać się z części teoretycznej i praktycznej.

Zakres **szkolenia** powinien obejmować następującą tematykę:

1. Czym jest cyberbezpieczeństwo i dlaczego jest istotne?
2. Największe wycieki danych w ostatnich 10 latach - omówienie przykładów
3. Kary nakładane na administratorów danych za wycieki danych
4. Wyjaśnienie podstawowych pojęć związanych z cyberbezpieczeństwem np.: https, AES-256, IP, TCP, domena, URL, komunikator i inne
5. Phishing i ransomware - zasady działania i rozpoznawania tych zagrożeń
6. Wyłudzenie danych osobowych za pomocą technik socjotechnicznych (phishing/vishing/smishing/spear phishing)
7. Jak bezpiecznie przetwarzać dane: szyfrowanie, przechowywanie, udostępnianie
8. Zasady korzystania z poczty elektronicznej
9. Bezpieczeństwo podczas korzystania z przeglądarek internetowych: Mozilla Firefox, Google Chrome, Microsoft Edge, Apple Safari
10. Bezpieczeństwo danych w chmurze
11. Prywatność w sieci czyli: trakery, ciastka, tryb incognito

12. Bezpieczeństwo pracy zdalnej - jak pracować zdalnie na sprzęcie własnym oraz służbowym?
13. Bezpieczeństwo zakupów oraz płatności w Internecie?
14. Fake news - identyfikacja i walka z fałszywymi wiadomościami
15. Czym jest socjotechnika i jak się przed nią bronić?

Oprócz szkolenia teoretycznego, Wykonawca powinien zrealizować **ćwiczenia praktyczne** obejmujące tematykę (np. w formie Quiz lub ćwiczenia):

1. Rozpoznawanie złośliwego oprogramowania i phishingu
2. Jak bezpiecznie komunikować się w Internecie?
3. Omówienie i prezentacja oprogramowania do obrony przed złośliwym oprogramowaniem:
    a) menadżer haseł (komercyjne vs open source)
    b) szyfrowanie danych na komputerze (komercyjne vs open source)
    c) szyfrowanie danych w chmurze (komercyjne vs open source)
4. Użytkowanie menadżera haseł, szyfrowanie danych
5. W jaki sposób zabezpieczyć własne dane?
6. Rozpoznawanie fałszywych informacji

V. Po zakończeniu szkolenia każdy z uczestników powinien otrzymać imienny certyfikat potwierdzający odbycie szkolenia.

VI. Szkolenie odbędzie się stacjonarnie w siedzibie Zamawiającego.

VII. Warunki postępowania:

Wykonawca posiada uprawnienia do wykonania określonej działalności lub czynności objętej niniejszym zapytaniem ofertowym,

Wykonawca posiada doświadczenie w realizacji szkoleń o wyżej wymienionej tematyce poparte referencjami z ostatnich dwóch lat. Referencje muszą dotyczyć osoby przeprowadzającej szkolenie.

VIII. Wraz ze złożoną ofertą, Wykonawca dostarczy **referencje oraz agendę szkolenia**.

IX. Czas realizacji: nie później niż do 14.08.2023

Termin zapłaty: 14 dni od daty poprawnie wystawionej i dostarczonej faktury na Gminę Ozimek.

Forma zapłaty: przelew na konto wykonawcy wskazane na fakturze.

Wymaga się spisania protokołu odbioru.

X. Postanowienia ogólne

1. Osoba do kontaktu ws. zamówienia: Barbara Durkalec- Sekretarz Gminy i Miasta w Ozimku tel. 602520041.
2. Kryteria wyboru ofert: Zamawiający nie dopuszcza składania ofert częściowych.
3. Za ofertę najkorzystniejszą uznana zostanie oferta najkorzystniejsza cenowo - cena 100%.
4. Ofertę należy przesłać: pocztą elektroniczną na adres sekretarz@ugim.ozimek.pl lub złożyć osobiście w zamkniętej kopercie, w siedzibie Zamawiającego ul. ks. Jana Dzierżona 4B, 46-040 Ozimek biuro podawcze, w terminie do 27 lipca 2023 roku do godz. 10:00.
5. Oferta winna być przygotowana na druku według Załącznika 1, podpisana i opieczętowana. Oferta powinna być czytelna i złożona w języku polskim. O terminie złożenia oferty, w tym również przesłanej pocztą, decyduje data wpływu do Zamawiającego. Oferty złożone po terminie nie będą rozpatrywane.
6. Z Wykonawcą, którego oferta zostanie wybrana, zostanie podpisana umowa, w miejscu i na warunkach określonych przez Zamawiającego. Informacja o wyborze Wykonawcy, miejscu, terminie podpisania umowy zostanie przekazana osobiście, e-mail lub pocztą tradycyjną Wykonawcy, którego ofertę wybrano.
7. Zamawiający zastrzega sobie prawo do odstąpienia bądź unieważnienia zapytania ofertowego bez

podawania przyczyn.

8. Zamawiający zastrzega sobie prawo do wzywania do wyjaśnień treści złożonej oferty w przypadku uzasadnionych wątpliwości co do jej treści po stronie Zamawiającego, na każdym etapie postępowania.

Załączniki:

1. Zał. nr 1 - formularz ofertowy

Z up. Burmistrza Ozimka

Barbara Durkalec

Sekretarz Gminy Ozimek

Realizacja projektu w ramach Umowy o powierzenie grantu o numerze 3413/1/2021 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT - EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina" o numerze P0PC.05.01.00-00-0001/21-00.

Pieczęć Wykonawcy

…….

Miejscowość, Data

FORMULARZ OFERTOWY S.271.16.2023.BD

na przeprowadzenie szkolenia pracowników Urzędu Gminy i Miasta w Ozimku i jednostek organizacyjnych z zakresu cyberbezpieczeństwa realizowane w ramach projektu „Cyfrowa Gmina”

Ja/My niżej podpisani oświadczam/y, że zrealizujemy w całości przedmiot zamówienia na warunkach opisanych w zapytaniu ofertowym w cenie: ..... zł brutto

(słownie .....).

……

Podpis Wykonawcy