

GMINA RYMANÓW**OPIS PRZEDMIOTU ZAMÓWIENIA****Znak sprawy FE.041.03.6.2025****Rymanów, dnia 21-08-2025r.**

Zamawiający: Gmina Rymanów
ul. Mitkowskiego 14A,
38-480 Rymanów
NIP: 6842377352, REGON: 370440590

ZAPYTANIE OFERTOWE W TRYBIE ZAMÓWIENIA PONIŻEJ 130.000 ZŁOTYCH

Gmina Rymanów zaprasza do składania ofert na wykonanie zadania o wartości szacunkowej nieprzekraczającej kwoty 130 tys. PLN (zwolnione ze stosowania ustawy Pzp na podstawie art. 2 ust. 1 pkt 1 ustawy z dnia 11 września 2019 roku Prawo zamówień publicznych - tekst jednolity Dz.U. z 202 r. poz. 13201129 z późn. zm.) pn.: „Przeprowadzenie audytu Bezpieczeństwa Informacji zgodnie z załącznikiem nr 6 do Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, Krajowego Systemu Cyberbezpieczeństwa (KSC), wykonanie Ankiety Dojrzałości oraz przygotowanie, dostosowanie i modyfikacja SZBI, dokumentacji ochrony danych osobowych, przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa i ochrony danych dla pracowników Urzędu Gminy w Rymanowie” realizowanego w ramach Projektu „Cyberbezpieczny Samorząd”.

Projekt finansowany w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021 — 2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa, projekt grantowy „Cyberbezpieczny Samorząd”, zgodnie z wytycznymi w zakresie kwalifikowalności wydatków w ramach Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności na lata 2021-2027.

Burmistrz Gminy Rymanów

(-)

Grzegorz Wołczański

(podpisane elektronicznie)

.....

I. Informacje o projekcie

Zamówienie jest finansowane w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021 - 2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa, projekt grantowy „Cyberbezpieczny Samorząd”.

Adres strony internetowej, na której jest prowadzone postępowanie i na której będą dostępne wszelkie dokumenty związane z prowadzoną procedurą:

<https://rymanow.bip.org.pl/przetargi/index/id/1>

Celem zamówienia jest podniesienie poziomu cyberbezpieczeństwa Zamawiającego poprzez Przeprowadzenie audytu Bezpieczeństwa Informacji zgodnie z załącznikiem nr 6 do Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności i Ankiety Dojrzałości, Krajowego Systemu Cyberbezpieczeństwa (KSC), oraz przygotowanie, dostosowanie i modyfikacja SZBI, dokumentacji ochrony danych osobowych, przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa i ochrony danych dla pracowników Urzędu Gminy w Rymanowie, zgodnie z najlepszymi praktykami oraz wymogami prawnymi.

II. Miejsce publikacji zapytania. Komunikacja z Zamawiającym

1. Wykonawca może złożyć tylko jedną ofertę.
2. Oferta winna odpowiadać treści Zapytania.
3. Komunikacja między Zamawiającym a Wykonawcami, w szczególności składanie ofert, wymiana informacji oraz przekazywanie dokumentów lub oświadczeń, odbywać się będzie przy użyciu środków komunikacji elektronicznej zapewnionych pod adresem: przetargi@rymanow.pl.
4. Adres strony internetowej: <https://rymanow.bip.org.pl/przetargi/index/id/1>
5. Ofertę należy złożyć w języku polskim wyłącznie za pośrednictwem poczty elektronicznej na adres przetargi@rymanow.pl **do 29 sierpnia 2025 r. do godziny 10⁰⁰**.
6. Złożoną ofertę należy zaszyfrować z podaniem hasła, aby Zamawiający mógł otworzyć ofertę po upływie terminu składania ofert (tj. **po godzinie 10⁰⁰ dnia 29 sierpnia 2025 r.**).
7. Otwarcie ofert nastąpi w dniu **29 sierpnia 2025 r. o godz. 10¹⁵**.
8. Ewentualne upoważnienie (pełnomocnictwo) innych osób do podpisania oferty wraz z załącznikami oraz do podpisania umowy musi być dołączone do oferty.
9. Upoważnienie (pełnomocnictwo), o którym mowa powyżej musi być podpisane przez osobę(y) uprawnioną(e) do reprezentowania firmy w obrocie prawnym.
10. Oferty złożone po terminie nie będą rozpatrywane.
11. Wykonawca przy użyciu środków komunikacji elektronicznej pod adresem: przetargi@rymanow.pl może przed upływem terminu składania ofert zmienić lub wycofać swoją ofertę.
12. Termin związania ofertą wynosi 30 dni. Bieg terminu rozpoczyna się wraz z upływem terminu składania ofert. Zamawiający zastrzega sobie możliwość wnioskowania o przedłużenie terminu związania ofertą o kolejne 30 dni.
13. Ceny należy podać z dokładnością do setnych części złotej tj. do dwóch miejsc po przecinku.

III. Przebieg postępowania

1. Zamawiający zastrzega sobie możliwość dokonania zmian w niniejszym Zapytaniu przed upływem terminu składania ofert.
2. W przypadku wprowadzenia zmian Zamawiający udostępni informację o zmianach na stronie internetowej prowadzonego postępowania <https://rymanow.bip.org.pl/przetargi/index/id/1>
3. Zamawiający może w toku badania i oceny ofert żądać od Wykonawców wyjaśnień dotyczących treści złożonych ofert oraz uzupełnienia dokumentów i oświadczeń, jeżeli takie były wymagane.
4. Wykonawca może zwrócić się do Zamawiającego przy użyciu środków komunikacji elektronicznej zapewnionych pod adresem: przetargi@rymanow.pl o wyjaśnienie treści Zapytania. W przypadku gdy wniosek wpłynie do Zamawiającego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert, wówczas Zamawiający udzieli odpowiedzi we wnioskowanym zakresie. Jeżeli wniosek wpłynie po ww. terminie, wówczas Zamawiający może udzielić wyjaśnień lub pozostawić wniosek bez rozpoznania.

Treść pytań (bez ujawniania źródła zapytania) wraz z wyjaśnieniami, Zamawiający opublikuje do wiadomości publicznej na stronie internetowej prowadzonego postępowania. W przypadku rozbieżności pomiędzy treścią Zapytania a treścią udzielonych odpowiedzi jako obowiązującą należy przyjąć treść pisma zawierającego późniejsze oświadczenie Zamawiającego.

5. Zamawiający odrzuci ofertę, która:
 - a. nie spełnia wymagań określonych w niniejszym Zapytaniu ofertowym,
 - b. zawiera błędy w obliczeniu ceny - Zamawiający może poprawić w treści oferty oczywiste omyłki pisarskie, oczywiste omyłki rachunkowe oraz inne omyłki polegające na niezgodności oferty z wymaganiami Zamawiającego, niepowodujące istotnych zmian w treści oferty - niezwłocznie zawiadamiając o tym Wykonawcę, którego oferta została poprawiona; w przypadku poprawienia innej omyłki polegającej na niezgodności oferty z wymaganiami Zamawiającego, niepowodującej istotnych zmian w treści oferty, oferta Wykonawcy podlega odrzuceniu, jeżeli Wykonawca nie wyrazi zgody na poprawienie oferty w terminie określonym przez Zamawiającego,
 - c. zawiera rażąco niską cenę w stosunku do przedmiotu zamówienia,
 - d. jest nieważna na podstawie odrębnych przepisów.
6. Wybór oferty i przekazanie przez Zamawiającego informacji o wyborze oferty nie stanowi przyjęcia oferty w rozumieniu Kodeksu cywilnego i nie oznacza zobowiązania do zawarcia umowy pomiędzy Zamawiającym i Wykonawcą.
7. Zawarcie umowy z wybranym Wykonawcą nastąpi w miejscu i terminie wyznaczonym przez Zamawiającego.
8. Jeżeli Wykonawca, którego oferta została wybrana uchyla się od zawarcia umowy, Zamawiający może wybrać najkorzystniejszą ofertę spośród pozostałych ofert, bez przeprowadzania ich ponownej oceny.
9. Niezwłocznie po zakończeniu postępowania zawiadamia się wszystkich Wykonawców, którzy złożyli oferty, o wyborze najkorzystniejszej oferty lub o unieważnieniu postępowania. W przypadku wyboru oferty najkorzystniejszej wskazuje się co najmniej imię i nazwisko lub nazwę (firmę) oraz adres Wykonawcy, którego ofertę wybrano oraz cenę wybranej oferty.
10. Złożenie oferty oznacza zaakceptowanie przez Wykonawcę wymagań zawartych w niniejszym Zapytaniu oraz zaakceptowanie ich bez zastrzeżeń.
11. Ze strony Zamawiającego osobami uprawnionymi do kontaktu w sprawie niniejszego postępowania są:
 - a. w sprawach proceduralnych: Zbigniew Chmiel, email: przetargi@rymanow.pl tel. 134355006 godziny pracy: od poniedziałku do piątku, w godz. 7:00 – 15:00
 - b. w sprawach dotyczących przedmiotu zamówienia: Grzegorz Sołtysik, e-mail: gsołtysik@rymanow.pl godziny pracy: od poniedziałku do piątku, w godz. 7:00 – 15:00.

IV. Opis przedmiotu zamówienia

Przedmiotem zamówienia jest: Przeprowadzenie audytu Bezpieczeństwa Informacji zgodnie z załącznikiem nr 6 do Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, Krajowego Systemu Cyberbezpieczeństwa (KSC), wykonanie Ankiety Dojrzałości oraz przygotowanie, dostosowanie i modyfikacja SZBI, dokumentacji ochrony danych osobowych, a także szkoleń z zakresu cyberbezpieczeństwa i ochrony danych dla pracowników Urzędu Gminy w Rymanowie.

Szkolenia:

Zakres zamówienia:

1) Udostępnienie i obsługa platformy e-learningowej:

Zamawiający wymaga, aby platforma spełniała następujące funkcjonalności:

- a) Możliwość założenia minimum 50 kont użytkowników z indywidualnym dostępem do przypisanych szkoleń oraz wglądem do własnych postępów.
- b) Dostęp administratorów do przeglądu aktywności użytkowników i grup użytkowników.
- c) Możliwość generowania certyfikatów ukończenia szkolenia dla każdego użytkownika.
- d) Dostęp do testów sprawdzających wiedzę.
- e) Możliwość zgłaszania zapytań merytorycznych oraz zgłoszeń technicznych przez użytkowników.
- f) Opcja samodzielnej zmiany hasła.
- g) Możliwość generowania raportów, zestawień statystycznych oraz automatycznego wysyłania wiadomości e-mail (informacyjnych, przypominających) na podstawie zadanych kryteriów.

Zawartość merytoryczna platformy:

Platforma powinna zawierać co najmniej 15 szkoleń e-learningowych z zakresu:

- a) Cyberbezpieczeństwa,
- b) Systemu Zarządzania Bezpieczeństwem Informacji (SZBI),
- c) Ochrony danych osobowych (RODO),

Grupy docelowe:

- a) Pracownicy JST,
- b) Kadra zarządzająca.

Tematyka szkoleń minimum 15:

- a) Podstawy prawne i wymagania dotyczące cyberbezpieczeństwa,
- b) Najpopularniejsze zagrożenia w cyberprzestrzeni,
- c) Typy ataków i metody obrony,
- d) Złośliwe oprogramowanie (malware),
- e) Phishing, spoofing i inne metody oszustw,
- f) Bezpieczne korzystanie z Internetu,
- g) Testy socjotechniczne,
- h) Ochrona fizyczna informacji,
- i) Praca zdalna i mobilna – dobre praktyki,
- j) Zasady tworzenia silnych haseł,
- k) Kryptografia,
- l) Zarządzanie incydentami,
- m) Zarządzanie ryzykiem,
- n) Ciągłość działania (ISO 22301),
- o) Normy ISO 27001 i ISO 27002:2022,
- p) SZBI – procedury i dokumentacja,
- q) RODO.

Każdy moduł szkoleniowy musi zawierać:

- a) Film szkoleniowy z lektorem w języku polskim (od 5 do 30 minut),
- b) Treści tekstowe,
- c) Test wiedzy.

Szkolenia stacjonarne

Wykonawca przeprowadzi szkolenia stacjonarne dla pracowników JST oraz kadry zarządzającej w tym kadry IT. Szkolenia powinny być jednodniowe i obejmować następujące bloki tematyczne:

Zakres dla pracowników oraz informatyków:

- a) Cyberbezpieczeństwo – definicje, obowiązki, akty prawne,
- b) Socjotechnika i rozpoznawanie zagrożeń (phishing, vishing, smishing, quishing),
- c) Ochrona fizyczna informacji w urzędzie i poza nim,
- d) Zarządzanie hasłami – dobre praktyki i narzędzia,
- e) Rozpoznawanie fałszywych witryn internetowych,
- f) Typowe ataki na samorządy i metody ochrony,

Moduły dodatkowe dla informatyków:

- a) SZBI zgodnie z ISO 27001:2023,
- b) Zarządzanie ryzykiem,
- c) Ciągłość działania (ISO 22301),
- d) Zarządzanie incydentami,
- e) Bezpieczeństwo sieci i analiza zagrożeń,
- f) Informatyka śledcza i testy penetracyjne,
- g) Ochrona systemów IT, analiza logów, kryptografia,

Moduły dodatkowe dla kadry zarządzającej:

- a) SZBI (ISO 27001:2023) – wdrażanie i nadzór,
- b) Zarządzanie ryzykiem,
- c) Ciągłość działania,
- d) Reagowanie na incydenty,

Wykonawca zrealizuje cykl zdalnych szkoleń dostępnych przez platformę e-learningową, obejmujących tematykę wskazaną w pkt. 2.2 i 2.3. Uczestnicy powinni mieć możliwość odbywania szkoleń w dogodnym czasie z dostępem do materiałów edukacyjnych i testów.

Symulator zagrożeń

W ramach usługi wykonawca udostępni moduł symulacji ataków phishingowych i spoofingowych, będący integralną częścią platformy e-learningowej. Funkcje wymagane:

- a) Wysyłanie przez administratorów spreparowanych wiadomości e-mail do wybranych użytkowników w celach edukacyjnych.
- b) Możliwość oceny reakcji użytkownika, m.in.:
 - Kliknięcie w niebezpieczny link,
 - Otwarcie nieautoryzowanego załącznika,
 - Podanie danych logowania na fałszywej stronie.

Wymagania dodatkowe

- a) Platforma oraz wszystkie materiały muszą być dostępne w języku polskim.
- b) Wszystkie szkolenia muszą być zgodne z obowiązującym stanem prawnym oraz aktualnymi normami ISO.
- c) Wykonawca zapewni wsparcie techniczne dla użytkowników i administratorów.
- d) Wykonawca powinien dysponować wsparciem co najmniej 2 osób posiadających status inżynierów technologii, w której została wykonana platforma e-learningowa oraz co najmniej jednego eksperta merytorycznego posiadającego stosowne uprawnienia określone w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. 2018 poz. 1999)

- e) Wykonawca powinien przedstawić certyfikaty lub równoważne dokumenty potwierdzające posiadanie stosownej wiedzy przez wskazanego eksperta oraz dokumentów (co najmniej listów referencyjnych wraz z opisami wcześniejszych usług np. audytów) potwierdzających posiadanie przez wskazanego eksperta min. 2-letniego doświadczenia w zakresie cyberbezpieczeństwa.
- f) Wykonawca powinien przedstawić dokumenty potwierdzające doświadczenie - co najmniej listy referencyjne wraz z opisami 3 wdrożeń platformy e-learningowej w ciągu ostatnich 3 lat (w tym co najmniej jednego wdrożenia dla 100 osób) oraz co najmniej jednego wdrożenia, które obejmowało zarówno szkolenia poprzez platformę jak i stacjonarne.

Termin realizacji:

Maksymalny termin realizacji zamówienia: 30 dni od dnia podpisania umowy.

System Zarządzania Bezpieczeństwem Informacji (SZBI)

Przedmiot zamówienia:

- a) Przedmiotem zamówienia jest:
 - 1) Przeprowadzenie audytu zgodności z Rozporządzeniem Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności (KRI),
 - 2) Opracowanie kompletnej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), zgodnej z normą PN-EN ISO/IEC 27001:2023.

Zakres zamówienia:

- 1) Audyt zgodności z Krajowymi Ramami Interoperacyjności (KRI)
 - Audyt obejmuje ocenę stopnia zgodności organizacji z wymaganiami zawartymi w Rozporządzeniu Rady Ministrów z dnia 21 maja 2024 r., Krajowym Systemie Cyberbezpieczeństwa (KSC), a w szczególności weryfikację spełnienia poniższych wymagań:
- 2) Zamieszczenie na stronie głównej i/lub BIP odesłań do opisów usług zawierających wymagane informacje (podstawa prawna, nazwa usługi, miejsce świadczenia, terminy, komórki odpowiedzialne), zgodnie z §5 ust. 2 pkt 1 i 4.
- 3) Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych zgodnie z wymaganiami dotyczącymi funkcjonalności, niezawodności, przenoszalności itp., z uwzględnieniem uznanych standardów (§15 ust. 1).
- 4) Udokumentowane zarządzanie usługami IT w oparciu o procedury, gwarantujące deklarowany poziom dostępności (§15 ust. 2).
- 5) Zapewnienie interoperacyjności systemów IT (komunikacja i szyfrowanie) zgodnie z §16 ust. 1.
- 6) Sposób udostępniania zasobów informatycznych (§18 ust. 1).
- 7) Przyjmowanie dokumentów elektronicznych przez systemy teleinformatyczne (§18 ust. 2).
- 8) Wdrożenie, utrzymanie i przegląd Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) – §19 ust. 1–14, w tym m.in.:
 - a) Aktualizacja regulacji wewnętrznych,
 - b) Inwentaryzacja sprzętu i oprogramowania,
 - c) Analiza ryzyka,
 - d) Zarządzanie uprawnieniami i ich aktualizacja
 - e) Szkolenia pracowników

- f) Zapewnienie ochrony informacji (monitorowanie, wykrywanie zagrożeń, zapobieganie)
 - g) Telepraca i praca mobilna
 - h) Zabezpieczenie informacji przed nieautoryzowanym dostępem
 - i) Postanowienia dotyczące bezpieczeństwa w umowach z dostawcami
 - j) Zarządzanie incydentami oraz ich raportowanie
 - k) Wewnętrzny audyt bezpieczeństwa informacji
 - Rezultatem audytu będzie raport końcowy zawierający opis stanu zgodności organizacji z wymaganiami KRI, identyfikację obszarów niezgodności oraz rekomendacje naprawcze.
 - Audyt musi zostać przeprowadzony przez osobę posiadającą certyfikaty zgodne z Rozporządzeniem Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzania audytów (Dz.U. 2018 poz. 1999).
-
- 9) Opracowanie i wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), przegląd opracowanie i wdrożenie dokumentacji ochrony danych osobowych
- 10) Wykonawca opracuje i dostarczy pełną dokumentację SZBI zgodną z normą PN-EN ISO/IEC 27001:2023, zgodną z obowiązującymi przepisami prawa aktualnymi na dzień zakończenia realizacji zadania, dostosowaną do charakteru działalności Zamawiającego.
- 11) Wykonawca opracuje i dostarczy pełną dokumentację ochrony danych osobowych zgodną z obowiązującymi przepisami prawa aktualnymi na dzień zakończenia realizacji zadania, dostosowaną do charakteru działalności Zamawiającego.
- 12) Dokumentacja powinna zawierać co najmniej:
- a) Politykę Bezpieczeństwa Informacji,
 - b) Zakres ról i odpowiedzialności,
 - c) Kontekst organizacji i strony zainteresowane,
 - d) Identyfikację zagrożeń i zarządzanie ryzykiem,
 - e) Procedury zarządzania incydentami,
 - f) Ewidencję aktywów informacyjnych
 - g) Klasyfikację i oznaczanie informacji,
 - h) Przesyłanie i udostępnianie informacji,
 - i) Zarządzanie tożsamością i kontrolą dostępu,
 - j) Bezpieczeństwo w relacjach z dostawcami i chmurą,
 - k) Wymagania dot. prywatności i ochrony danych osobowych (PII),
 - l) Ciągłość działania (BCP),
 - m) Zarządzanie podatnościami, konfiguracją i zmianami,
 - n) Zarządzanie bezpieczeństwem aplikacji, sieci, zasobów fizycznych,
 - o) Wykorzystanie kryptografii,
 - p) Zapobieganie wyciekom danych,
 - q) Zapewnienie zgodności z wymaganiami prawnymi i umownymi,
 - r) Procedury eksploatacyjne i monitorujące,
 - s) Zasady pracy zdalnej i korzystania z urządzeń mobilnych,
 - t) Działania zapobiegające złośliwemu oprogramowaniu,
 - u) Procedury audytowe,
 - Dokumentacja powinna być przygotowana w formie umożliwiającej wdrożenie systemu oraz jego dalszą certyfikację zgodnie z wymaganiami ISO 27001:2023.

Wymagania dodatkowe:

- Wykonawca zapewni kompleksowe wykonanie zadania w języku polskim.

- Wszelkie opracowania muszą uwzględniać aktualny stan prawny i obowiązujące normy.
- W przypadku wykrycia niezgodności, Wykonawca proponuje środki naprawcze.
- Raport z audytu powinien zawierać opis stanu zgodności z przepisami, listę uchybień oraz propozycje działań korygujących.
- Wykonawca powinien dysponować co najmniej jedną osobą posiadającą uprawnienia określone w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. 2018 poz. 1999)

Rezultaty realizacji zamówienia:

- Raport z audytu KRI,
- Kompletna dokumentacja SZBI zgodna z ISO/IEC 27001:2023 (aktualna na dzień zakończenia wykonania zadania- maksymalnie do dnia 31.12.2025 r.)
- Kompletna dokumentacja ochrony danych osobowych zgodna z obowiązującymi przepisami prawa (aktualna na dzień zakończenia wykonania zadania- maksymalnie do dnia 31.12.2025 r.)
- Lista rekomendacji i zaleceń dostosowawczych
- Aktualizacja stanu dokumentacji na dzień 30.06.2026 r.
- Nagrane szkolenia pozostają własnością zamawiającego,
- Platforma lerningowa funkcjonuje co najmniej przez okres do czasu zakończenia trwania projektu (tj. dnia).

Termin realizacji zamówienia:

Realizacja przedmiotu zamówienia powinna nastąpić w terminie:

- Wykonanie audytu oraz przygotowanie dokumentacji SZBI nie później niż do dnia 31 grudnia – zakończenie i rozliczenie zadania
- Wykonanie szkoleń i przygotowanie platformy szkoleniowej nie później niż do dnia 31 grudnia – zakończenie i rozliczenie zadania
- nie dłuższym niż 120 dni kalendarzowych od dnia podpisania umowy dla SZBI oraz 30 dni dla audytu KRI. (UWAGA WN – SZBI to powinno być 4 m-ce , audyt może mieć znacznie krótszy termin – przyjmuje się 30 dni)

V. Kody CPV

79212000-3: Usługi audytu

80510000-2: Usługi szkolenia specjalistycznego

80420000-4: Usługi e-learning

VI. Warunki udziału w postępowaniu.

1. o udzielenie zamówienia mogą ubiegać się Wykonawcy:
 - a. którzy złożą oświadczenie (zgodnie z Załącznikiem nr 2), że nie podlegają wykluczeniu z postępowania oraz akceptują warunki określone w niniejszym Zapytaniu Ofertowym
 - b. którzy posiadają zdolność techniczną lub zawodową do wykonania zamówienia.
2. Przesłanie oferty w odpowiedzi na niniejsze Zapytanie ofertowe jest jednoznaczne ze złożeniem oświadczenia, że Wykonawca spełnia powyższe kryteria.
3. Złożenie oferty jest jednoznaczne z zapoznaniem się z treścią zapytania ofertowego i akceptacją warunków realizacji zamówienia określonych w niniejszym Zapytaniu Ofertowym.
4. Zamawiający informuje, że niniejsze zapytanie ofertowe nie stanowi oferty zawarcia umowy, ani też oferty prowadzenia negocjacji w tym celu i jest skierowane do wielu adresatów.

VII. Termin wykonania zamówienia i warunki płatności

1. Wykonawca wykona przedmiot zamówienia w terminie 14 dni od dnia zawarcia Umowy.
2. Zapłata za wykonany przedmiot zamówienia nastąpi po przekazaniu prawidłowo wykonanego przedmiotu zamówienia na podstawie faktury VAT wystawionej przez Wykonawcę, w terminie 14 dni od dnia jej doręczenia Zamawiającemu z zastrzeżeniem ust. 3. poniżej.
3. Podstawą dokonania zapłaty będzie Protokół zdawczo - odbiorczy prawidłowo wykonanego przedmiotu zamówienia, załącznik nr 4 do zapytania ofertowego, stwierdzający kompletność i zgodność wykonania przedmiotu zamówienia oraz poprawnie wystawiona faktura VAT.
4. Dane do faktury:
NABYWCA:
Gmina Rymanów
ul. Mitkowskiego 14A
38-480 Rymanów
NIP: 6842377352
REGON: 370440590

VIII. Kryteria wyboru najkorzystniejszej oferty

1. Zamawiający podczas wyboru najkorzystniejszej oferty będzie kierował się kryterium 100% cena.

IX. Klauzula informacyjna RODO

1. Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. I), dalej „RODO”, informuję, że:
 - a. administratorem Pani/Pana danych osobowych jest Gmina Rymanów, ul. Mitkowskiego 14A, 38-480 Rymanów, e-mail: gmina@rymanow.pl, tel.: 134355006,
 - b. administrator wyznaczył Inspektora Danych Osobowych, z którym można się kontaktować pod adresem, e-mail: iod@rymanow.pl,
 - c. Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego pn.: „Przeprowadzenie audytu Bezpieczeństwa Informacji zgodnie z załącznikiem nr 6 do Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, Krajowego Systemu Cyberbezpieczeństwa (KSC), wykonanie Ankiety Dojrzałości oraz przygotowanie, dostosowanie i modyfikacja SZBI, dokumentacji ochrony danych osobowych, przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa i ochrony danych dla pracowników Urzędu Gminy w Rymanowie”,
 - d. odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o ustawę z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2020 roku, poz. 2176 z późn. zm.),
 - e. Pani/Pana dane osobowe będą przechowywane przez okres trwałości Projektu „Cyberbezpieczny Samorząd”,
 - f. obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem wynikającym z procedur udzielania zamówień w związku z realizacją umów w podlegających dofinansowaniu w ramach w/w Projektu,
 - g. w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO,

- h. posiada Pani/Pan:
 - 1. na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących,
 - 2. na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych,
 - 3. na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO¹,
 - 4. prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
- i. nie przysługuje Pani/Panu:
 - 1 w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych,
 - 2 prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO,
 - 3 na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

X. Lista załączników

- 1. Załącznik nr 1 - Formularz ofertowo-cenowy
- 2. Załącznik nr 2 - Oświadczenie
- 3. Załącznik nr 3 - Wzór Umowy
- 4. Załącznik nr 4 - Protokół odbioru końcowego
- 5. Załącznik nr 5 - Klauzula informacyjna FERC

¹ prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii europejskiej lub państw członkowskich.