ZAPYTANIE OFERTOWE

Znak sprawy: USC.EL.271.1.2026 Ceków-Kolonia, dnia 14-07-2026 r.

Zamówienie realizowane w ramach projektu grantowego “Cyberbezpieczny Samorząd” Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 - Wzmocnienie krajowego systemu cyberbezpieczeństwa

Numer umowy o powierzenie grantu: FERC.02.02-CS.01-001/23/2399/FERC.02.02-CS.01-001/23/2024

GMINA CEKÓW-KOLONIA

Ceków-Kolonia 51, 62-834 Ceków Wójt Gminy: Mariusz Chojnacki

Osoby do kontaktu:

- Janusz Frątczak (Sekretarz Gminy), e-mail: sekretarz@cekow.pl, tel. 734 443 869
- Łukasz Skórzewski, e-mail: ewidencja@cekow.pl, tel. 692 083 471

I. PODSTAWA PRAWNA I TRYB UDZIELENIA ZAMÓWIENIA

Niniejsze zapytanie ofertowe prowadzone jest z wyłączeniem przepisów ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (t.j. Dz.U. z 2026 r. poz. 793 ze zm.) na podstawie art. 2 ust. 1 pkt 1 tej ustawy, z uwagi na wartość zamówienia nieprzekraczającą kwoty 170 000 złotych netto.

Postępowanie prowadzone jest zgodnie z zasadą konkurencyjności wynikającą z wytycznych dotyczących kwalifikowalności wydatków w ramach projektu grantowego “Cyberbezpieczny Samorząd”, realizowanego w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2 - Wzmocnienie krajowego systemu cyberbezpieczeństwa.

II. INFORMACJE OGÓLNE

Celem projektu jest zwiększenie poziomu bezpieczeństwa informacji jednostek samorządu terytorialnego poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych.

Urząd Gminy Ceków-Kolonia, działając w imieniu własnym oraz w imieniu podległych jednostek organizacyjnych, zaprasza do złożenia oferty na realizację usług opisanych w niniejszym zapytaniu ofertowym.

Zamówienie finansowane jest w ramach grantu przyznanego Gminie Ceków-Kolonia na podstawie umowy o powierzenie grantu nr FERC.02.02-CS.01.001/23/2399/FERC.02.02-CS.01-001/23/2024. Grantodawcą jest Skarb Państwa, w imieniu którego działa Centrum Projektów Polska Cyfrowa z siedzibą w Warszawie, ul. Spokojna 13A.

III. OPIS ZAMAWIAJĄCEGO I JEDNOSTEK ORGANIZACYJNYCH

Zamówienie dotyczy czterech odrębnych podmiotów, które będą fakturowane osobno:

Lp.	Nazwa jednostki	NIP
1.	Urząd Gminy Ceków-Kolonia (dalej: UG)	9680371377
2.	Gminny Ośrodek Pomocy Społecznej w Cekowie-Kolonii (dalej: GOPS)	9680770226
3.	Gminne Centrum Promocji Kultury, Sportu i Rekreacji w Cekowie-Kolonii (dalej: GCPKSiR)	9680973834
4.	Gminny Zespół Obsługi Administracyjnej i Ekonomicznej Oświaty w Cekowie-Kolonii (dalej: GZOAEO)	9680000451

Wszystkie podmioty posiadają wspólną siedzibę pod adresem: Ceków-Kolonia 51, 62-834 Ceków.

IV. OPIS INFRASTRUKTURY INFORMATYCZNEJ

Urząd Gminy i wszystkie jednostki organizacyjne korzystają ze wspólnej infrastruktury informatycznej, w skład której wchodzą:

Infrastruktura wspólna:

- 2 serwery (serwerownia zlokalizowana w jednym pomieszczeniu)
- System backupu
- Monitoring zewnętrzny budynku
- System alarmowy
- Agregat prądotwórczy

Urząd Gminy Ceków-Kolonia:

- 18 komputerów stacjonarnych
- 9 laptopów
- 12 telefonów służbowych z systemem Android

Gminny Ośrodek Pomocy Społecznej:

- 7 komputerów stacjonarnych
- 1 laptop
- 4 telefony służbowe z systemem Android

Gminne Centrum Promocji Kultury, Sportu i Rekreacji:

- 2 komputery stacjonarne
- 1 telefon służbowy z systemem Android

Gminny Zespół Obsługi Administracyjnej i Ekonomicznej Oświaty:

- 4 komputery stacjonarne

- 1 telefon służbowy z systemem Android

V. PRZEDMIOT ZAMÓWIENIA

Kompleksowe usługi audytorsko-wdrożeniowe w zakresie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) dla Urzędu Gminy, zgodnie z wymaganiami ISO/IEC 27001, Krajowych Ram Interoperacyjności (KRI) oraz RODO i KSC.

1. Cel i zakres zamówienia

Przedmiotem zamówienia jest świadczenie kompleksowych usług doradczych, audytorskich oraz wdrożeniowych mających na celu opracowanie, wdrożenie, weryfikację i dostosowanie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w Urzędzie Gminy oraz pozostałych wymienionych jednostkach do obowiązujących wymogów prawnych oraz normatywnych. Usługa ma na celu zagwarantowanie najwyższego poziomu poufności, integralności i dostępności przetwarzanych danych, ze szczególnym uwzględnieniem danych osobowych mieszkańców oraz wrażliwej infrastruktury teleinformatycznej urzędu.

Realizacja zamówienia musi uwzględniać specyfikę funkcjonowania jednostek sektora finansów publicznych i samorządu terytorialnego, w tym ograniczenia budżetowe, strukturę organizacyjną (podział na referaty) oraz specyficzne systemy dziedzinowe i rejestry publiczne.

2. Szczegółowy zakres rzeczowy zamówienia

Zadanie 1. Opracowanie i wdrożenie kompletnej dokumentacji SZBI

Wykonawca zobowiązany jest do opracowania i wdrożenia spójnego, zintegrowanego pakietu dokumentacji SZBI dostosowanego do struktury urzędu gminy i jednostek organizacyjnych, specyfiki systemów dziedzinowych oraz wymagań normatywnych. Dokumentacja musi uwzględniać następujące elementy nadrzędne i operacyjne:

- Polityka Bezpieczeństwa Informacji Urzędu Gminy (PBI) – dokument wysokopoziomowy deklarujący cele i zaangażowanie kierownictwa.
- Procedura identyfikacji wymagań prawnych, branżowych i umownych wraz z dedykowanym Rejestrem wymagań specyficznych dla samorządu.
- Metodyka szacowania ryzyka dostosowana do specyfiki jednostek publicznych (w oparciu o ISO 27005/ISO 31000) wraz z gotowym Rejestrem Ryzyk i Planem Postępowania z Ryzykiem.
- Deklaracja Stosowania (SoA - Statement of Applicability) – uwzględniająca pełny wykaz 93 zabezpieczeń normy PN-EN ISO/IEC 27001:2023-08, ze wskazaniem środków wdrożenia i uzasadnieniem wyłączeń.
- Polityka Kontroli Dostępu i Zarządzania Tożsamością – w tym procedury nadawania, przeglądu i odbierania uprawnień użytkowników i administratorów.
- Polityka Zarządzania Kopiami Zapasowymi – określająca harmonogramy, retencję, przechowywanie off-site oraz procedury i protokoły testowych odtworzeń.
- Procedura Zarządzania Incydentami i Naruszeniami Bezpieczeństwa – w tym instrukcje triage'u, playbooki reakcji na zagrożenia, Dziennik Incydentów oraz wzory notyfikacji do właściwych organów (UODO, CSIRT w terminie do 24h/72h).

- Polityka Bezpieczeństwa Fizycznego i Środowiskowego – określająca granice stref chronionych (np. kasy, archiwa, referat spraw obywatelskich/dowodów osobistych, serwerownia), zasady wejść osób trzecich/gości oraz nadzoru nad kluczami, Powinny zawierać również procedury dotyczące monitoringu, systemu alarmowego i zasilania awaryjnego.
- Polityka Bezpieczeństwa w Relacjach z Dostawcami – w tym instrukcje weryfikacji ze szczególnym uwzględnieniem due diligence dostawców systemów IT i asysty technicznej oraz wzorce standardowych klauzul bezpieczeństwa (NDA, RODO, SLA).
- Regulamin Pracy Zdalnej i Bezpieczeństwa Urządzeń Mobilnych (BYOD) – regulujący zasady ochrony danych w Home Office i podczas pracy w terenie (szyfrowanie stacji, bezpieczne tory VPN, dwuskładnikowe uwierzytelnianie MFA).

Wdrożenie powinno obejmować co najmniej następujące kroki:

1. Ogłoszenie SZBI oraz wewnętrzne opublikowanie dokumentacji SZBI.
2. Przeprowadzenie szkoleń z zakresu SZBI (szkolenia z zakresu SZBI przeprowadzone zostaną w odrębnym postępowaniu jednak przed wykonaniem audytu powdrożeniowego) :
    a. Dla wszystkich pracowników – role i zadania w SZBI
    b. Dla kierownictwa i osób o szczególnym znaczeniu dla SZBI – zarządzanie strategiczne cyberbezpieczeństwem i ciągłością działania.
3. Inwentaryzacja i klasyfikacja aktywów informacyjnych
4. Wybór adekwatnych do zagrożeń zabezpieczeń z aneksu A normy ISO/IEC27001
5. Stworzenie Deklaracji Stosowania (SoA)

Zadanie 2. Przegląd aktualnie posiadanych polityk bezpieczeństwa i ich aktualizacja

Wykonawca dokona szczegółowego przeglądu i inwentaryzacji wszystkich aktualnie funkcjonujących w Urzędzie Gminy i pozostałych jednostkach regulacji wewnętrznych (np. Polityki Bezpieczeństwa Informacji, Instrukcji Zarządzania Systemem Informatycznym, Regulaminów Pracy, dokumentacji RODO itp.) pod kątem ich zgodności merytorycznej, prawnej i terminologicznej. Zadanie obejmuje:

- Analizę zgodności (Gap Analysis) obecnej dokumentacji z nową edycją normy PN-EN ISO/IEC 27001:2023-08 i nowym podziałem zabezpieczeń (93 zabezpieczenia zamiast dawnych 114).
- Dostosowanie zapisów do aktualnego stanu prawnego, w tym uwzględnienie Ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz.U. 2026 poz. 252) (NIS2), Rozporządzenia o Krajowych Ramach Interoperacyjności z 2024 roku (Dz.U. 2024 poz. 773), 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) czyli tzw. Ogólnego Rozporządzenia o Ochronie Danych Osobowych (RODO), wytycznych Urzędu Ochrony Danych Osobowych (UODO) oraz tzw. dobrych praktyk w zakresie stosowania międzynarodowej normy ISO/IEC 27001.
- Identyfikację martwych procedur, niespójności terminologicznych (np. odwołania do nieistniejących ról, brak rozliczalności) oraz pustych placeholderów i szablonów roboczych.
- Opracowanie spójnego planu aktualizacji, scalenia lub wycofania poszczególnych dokumentów w celu uniknięcia nadmiarowości biurokratycznej (tzw. 'odchudzenie' i uproszczenie systemu).

- Przeprowadzenie warsztatów uzgodnieniowych z kluczowymi osobami w Urzędzie (np. Sekretarz Gminy, Informatyk, Inspektor Ochrony Danych) w celu wypracowania ostatecznych, wykonalnych wersji dokumentów.

Zadanie 3. Audyt wstępny (przedwdrożeniowy)

Celem audytu wstępnego jest identyfikacja stanu faktycznego (Baseline) zabezpieczeń organizacyjnych, fizycznych i technicznych w Urzędzie Gminy i pozostałych jednostkach oraz mapowanie luk przed przystąpieniem do prac projektowych i wdrożeniowych. Zakres audytu obejmuje:

- Weryfikację obszaru organizacyjnego: przegląd ról, podziału obowiązków, świadomości personelu, procesów rekrutacji i onboardingu.
- Weryfikację bezpieczeństwa fizycznego: ocena stref dostępu, fizycznych granic urzędu, systemów alarmowych, monitoringu CCTV, zabezpieczeń przeciwpożarowych oraz niszczenia nośników papierowych.
- Weryfikację bezpieczeństwa teleinformatycznego (IT): przegląd topologii sieci, konfiguracji zapór sieciowych (firewall), zasad segmentacji sieci, procedur backupu, aktualizacji (patching), ochrony antywirusowej (AV/EDR), zarządzania tożsamością i hasłami.
- Skanowanie podatności infrastruktury sieciowej i serwerów Urzędu Gminy (np. z użyciem certyfikowanych narzędzi) w celu identyfikacji krytycznych luk bezpieczeństwa.
- Opracowanie formalnego Raportu z Audytu Wstępnego zawierającego pełną listę zidentyfikowanych podatności, ocenę poziomu zgodności z Krajowymi Ramami Interoperacyjności (§ 20 KRI) oraz RODO i normą ISO 27001, wraz z rekomendacjami naprawczymi.

Zadanie 4. Audyt powdrożeniowy (zgodności)

Audyt powdrożeniowy (audyt zgodności z wymaganiami KRI oraz normą ISO 27001) ma na celu obiektywną weryfikację skuteczności i stopnia przyswojenia wdrożonych procedur oraz mechanizmów bezpieczeństwa przez Urząd Gminy i pozostałe jednostki. Audyt ten stanowi formalne wypełnienie obowiązku wynikającego bezpośrednio z § 20 ust. 2 pkt 14 Rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności i obejmuje:

- Weryfikację funkcjonowania i przestrzegania wdrożonych polityk w praktyce codziennej (testy próbkowania, wywiady z pracownikami na różnych szczeblach, obserwacja bezpośrednia – np. testy 'czystego biurka').
- Weryfikację techniczną: sprawdzenie, czy konfiguracje IT (np. GPO Active Directory, uprawnienia sieciowe, harmonogramy backupów, logowanie zdarzeń) odpowiadają sformalizowanym procedurom.
- Weryfikację dowodową: przegląd wygenerowanych w systemie rejestrów (np. Rejestru uprawnień, Dziennika incydentów, Protokołów testowych odtworzeń backupów, Rejestru wejść do serwerowni).
- Opracowanie i dostarczenie formalnego Raportu z Audytu Powdrożeniowego (zgodności z KRI i ISO/IEC 27001) podpisanego przez uprawnionego Audytora Wiodącego. Raport musi jednoznacznie określać poziom zgodności, stwierdzone niezgodności (poważne i drobne), spostrzeżenia oraz rekomendacje dla pętli ciągłego doskonalenia (PDCA).

VI. Wymagania wobec Wykonawcy

W celu zagwarantowania należytej staranności oraz rzetelności realizowanych zadań, Wykonawca musi wykazać, że dysponuje zespołem ekspertów posiadających udokumentowane kwalifikacje i doświadczenie:

1. Dysponowanie osobami posiadającymi kwalifikacje w zakresie bezpieczeństwa informacji i/lub audytu SZBI, a w szczególności:

- Co najmniej jedną osobą posiadającą certyfikat Audytora Wiodącego SZBI wg PN-EN ISO/IEC 27001:2022 wydany przez jednostkę akredytowaną przez PCA zgodnie z normą PN-EN ISO/IEC 17024, ujęty w wykazie certyfikatów uprawniających do przeprowadzenia audytu zgodnie z rozporządzeniem Ministra Cyfryzacji z dnia 12 października 2018 r. (Dz.U. poz. 1560) - wymagane do realizacji Zadania 4;
- Co najmniej jedną osobą posiadającą certyfikat Audytora Wiodącego lub Audytora Wewnętrznego SZBI wg PN-EN ISO/IEC 27001:2022 wydany przez jednostkę akredytowaną przez PCA zgodnie z normą PN-EN ISO/IEC 17024 - wymagane do realizacji Zadania 3.
- Co najmniej 1 osoba w zespole wykonującym zamówienie posiadająca certyfikat Audytora Wewnętrznego normy ISO/IEC 27701 (Zarządzanie prywatnością) - wymagane do realizacji Zadania 3.
- Udokumentowane wykazanie przeprowadzenia w okresie ostatnich 3 lat co najmniej 3 audytów bezpieczeństwa informacji lub wdrożeń SZBI w jednostkach administracji publicznej (Urząd Gminy, Urząd Miasta, Starostwo Powiatowe) potwierdzających znajomość specyfiki samorządowej
- Znajomość specyfiki prawa ochrony danych osobowych potwierdzona wykształceniem wyższym (magisterskie lub licencjat) lub podyplomowym w zakresie ochrony danych osobowych przynajmniej jednej osoby w zespole.
- Znajomość zagadnień dotyczących cyberbezpieczeństwa potwierdzona wykształceniem wyższym (magisterskie, inżynierskie lub licencjat) lub podyplomowym w zakresie cyberbezpieczeństwa przynajmniej jednej osoby w zespole.

VII. WARUNKI REALIZACJI

1. Wycena powinna być przygotowana odrębnie dla każdej z czterech jednostek.

2. Faktury będą wystawiane odrębnie na każdą z jednostek, zgodnie z numerami NIP wskazanymi w rozdziale III.

3. Zamawiający oczekuje podania cen netto i brutto dla każdego zadania i każdej jednostki osobno.

4. Wykonawca powinien wskazać proponowany harmonogram realizacji zamówienia.

5. Zamawiający dopuszcza złożenie jednej oferty obejmującej wszystkie cztery jednostki z wyraźnym podziałem na poszczególne podmioty.

6. Realizacja zamówienia finansowana jest ze środków projektu grantowego “Cyberbezpieczny Samorząd” (umowa nr FERC.02.02-CS.01.001/23/2399/FERC.02.02-CS.01-001/23/2024), co wiąże się z koniecznością przedłożenia przez Wykonawcę

dokumentacji potwierdzającej prawidłowe wykonanie zamówienia na potrzeby rozliczenia grantu.

7. Wykonawca wyraża zgodę na udostępnienie wszelkiej dokumentacji związanej z realizacją zamówienia instytucjom uprawnionym do kontroli, w szczególności Centrum Projektów Polska Cyfrowa oraz innym podmiotom upoważnionym do kontroli realizacji projektu grantowego.

8. Nieprzekraczalny termin zakończenia audytu powdrożeniowego dla wszystkich jednostek: 15 września 2026 r. Wymóg ten jest warunkiem koniecznym przyjęcia oferty do oceny.

VIII. KRYTERIA WYBORU OFERTY

Zamawiający dokona wyboru najkorzystniejszej oferty na podstawie następujących kryteriów oceny:

Lp.	Kryterium	Waga
1.	Cena (C)	55%
2.	Termin realizacji (T)	30%
3.	Doświadczenie Wykonawcy (D)	15%

1. Kryterium ceny (C) - waga 55 punktów
Punkty za kryterium ceny obliczane są według wzoru:

C = (Cena minimalna spośród złożonych ofert / Cena oferty badanej) x 55

Za cenę oferty przyjmuje się łączną cenę brutto za realizację zamówienia dla wszystkich czterech jednostek łącznie. W przypadku ofert składanych tylko dla wybranych jednostek porównanie następuje w odniesieniu do ceny za tę samą jednostkę lub jednostki.

2. Kryterium terminu realizacji (T) - waga 30 punktów

Punkty za kryterium terminu realizacji obliczane są według wzoru:

T = (Termin minimalny spośród złożonych ofert / Termin oferty badanej) x 30

Termin realizacji należy podać w dniach kalendarzowych, liczonych od dnia podpisania umowy do dnia przekazania kompletnej dokumentacji powdrożeniowej wraz z raportem z audytu powdrożeniowego. Termin zakończenia audytu powdrożeniowego nie może w żadnym przypadku przekroczyć dnia 15 września 2026 r.

3. Kryterium doświadczenia Wykonawcy (D) - waga 15 punktów

Punkty za kryterium doświadczenia przyznawane są na podstawie liczby zrealizowanych zamówień dotyczących opracowania lub wdrożenia SZBI dla jednostek sektora publicznego, według następującej tabeli:

Liczba udokumentowanych zamówień zrealizowanych dla jednostek sektora publicznego	Liczba punktów
3 zamówienia	10

Liczba udokumentowanych zamówień zrealizowanych dla jednostek sektora publicznego	Liczba punktów
4 zamówienia i więcej	15

Przez jedno zamówienie rozumie się odrębną umowę zawartą z jednym zamawiającym, dotyczącą opracowania lub wdrożenia dokumentacji SZBI. Wykonawca zobowiązany jest wskazać nazwę zamawiającego, zakres zamówienia oraz rok jego realizacji. Zamawiający zastrzega sobie prawo do weryfikacji wskazanego doświadczenia.

Łączna punktacja

Suma punktów = C + T + D (maksymalnie 100 punktów)

Za najkorzystniejszą zostanie uznana oferta, która uzyska najwyższą łączną liczbę punktów. W przypadku uzyskania przez dwie lub więcej ofert takiej samej łącznej liczby punktów, Zamawiający wezwie tych Wykonawców do złożenia ofert dodatkowych w zakresie kryterium ceny.

IX. TERMIN I SPOSÓB ZŁOŻENIA OFERTY

1. Wypełniony formularz oferty (odrębny dla każdej jednostki) należy przesłać w terminie do dnia 21-07-2026 r. na adres e-mail: sekretarz@cekow.pl lub ewidencja@cekow.pl.

2. W tytule wiadomości należy wpisać: “Zapytanie ofertowe SZBI - [nazwa jednostki]”.

3. Oferty złożone po terminie nie będą rozpatrywane.

4. Wykonawca jest związany złożoną ofertą przez okres 30 dni od upływu terminu składania ofert.

5. Zamawiający zastrzega sobie prawo do unieważnienia postępowania bez podania przyczyny, w szczególności w przypadku, gdy ceny złożonych ofert przekroczą kwotę, jaką Zamawiający może przeznaczyć na sfinansowanie zamówienia.

6. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.

Pytania dotyczące przedmiotu zamówienia należy kierować do:

- Janusz Frątczak, tel. 734 443 869, e-mail: sekretarz@cekow.pl
- Łukasz Skórzewski, tel. 692 083 471, e-mail: ewidencja@cekow.pl

X. INFORMACJE DODATKOWE

1. Zamawiający zastrzega sobie możliwość negocjacji ceny z Wykonawcą, który złożył najkorzystniejszą ofertę.

2. Wyniki postępowania zostaną przekazane wszystkim Wykonawcom, którzy złożyli ofertę, drogą elektroniczną.

3. Niniejsze zapytanie ofertowe zamieszczone zostaje publicznie w celu zapewnienia zasady konkurencyjności wymaganej przy realizacji projektów dofinansowanych ze środków Unii Europejskiej.

1. Projekt współfinansowany jest ze środków Unii Europejskiej w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027.

Mariusz Chojnacki

Wójt Gminy Ceków-Kolonia

Signature Not Verified

Dokument podpisany przez
Mariusz Chojnacki; Urząd
Gminy Ceków Kolonia
Data: 2026.07.15 08:38:18 CEST

FORMULARZ OFERTY NR 1

URZĄD GMINY CEKÓW-KOLONIA

Zapytanie ofertowe nr USC.EL.271.1.1.2026

DANE WYKONAWCY:

Nazwa firmy / imię i nazwisko: …….

Adres: …….

NIP: …….

REGON: …….

Osoba do kontaktu: …….

Telefon: …….

E-mail: …….

ZAMAWIAJĄCY: Urząd Gminy Ceków-Kolonia, Ceków-Kolonia 51, 62-834 Ceków
NIP Urzędu Gminy: 9680371377

TABELA WYCENY

Lp.	Zakres usługi	Cena netto (zł)	Stawka VAT (%)	Cena brutto (zł)
1.	Audyt wstępny (przedwdrożeniowy) - analiza luk, inwentaryzacja aktywów, ocena stanu bezpieczeństwa			
2.	Przegląd aktualnie posiadanych polityk bezpieczeństwa informacji i ocena ich zgodności z obowiązującymi przepisami			
3.	Opracowanie dokumentacji SZBI (polityki, procedury, instrukcje, rejestry) dostosowanej do specyfiki Urzędu Gminy			
4.	Wdrożenie dokumentacji SZBI (wprowadzenie zarządzeń, wsparcie przy wdrożeniu procedur operacyjnych)			

Lp.	Zakres usługi	Cena netto (zł)	Stawka VAT (%)	Cena brutto (zł)
5.	Audyt powdrożeniowy - weryfikacja wdrożenia, identyfikacja niezgodności, działania korygujące			
	RAZEM			

Infrastruktura objęta zamówieniem (Urząd Gminy):

- 2 serwery (wspólne z jednostkami organizacyjnymi)
- 18 komputerów stacjonarnych
- 9 laptopów
- 12 telefonów służbowych z systemem Android
- System backupu, monitoring zewnętrzny, system alarmowy, agregat prądotwórczy

Proponowany harmonogram realizacji:

Audyt wstępny: od …….. do ……..

Przegląd i aktualizacja polityk: od …….. do ……..

Opracowanie dokumentacji SZBI: od …….. do ……..

Wdrożenie dokumentacji SZBI: od …….. do ……..

Audyt powdrożeniowy: od …….. do …….. (nieprzekraczalnie do 15.09.2026 r.)

Łączny termin realizacji zamówienia (w dniach kalendarzowych od dnia podpisania umowy): …….. dni

Informacja dotycząca audytu

Audyt wstępny i powdrożeniowy zostanie przeprowadzony przez: (zaznaczyć właściwe)

[ ] Wykonawcę we własnym zakresie

[ ] Podmiot zewnętrzny działający na zlecenie Wykonawcy

Jeżeli przez podmiot zewnętrzny - nazwa i dane podmiotu:

……

Kwalifikacje i certyfikaty osób przeprowadzających audyt

Audyt wstępny (Zadanie 3) - osoba przeprowadzająca audyt:

Imię i nazwisko: …….

Posiadany certyfikat (zaznaczyć właściwe):

[ ] Certyfikat Audytora Wiodącego SZBI wg PN-EN ISO/IEC 27001:2022 wydany przez akredytowaną jednostkę certyfikującą

[ ] Certyfikat Audytora Wewnętrznego SZBI wg PN-EN ISO/IEC 27001:2022 wydany przez akredytowaną jednostkę certyfikującą

Nazwa jednostki certyfikującej: …….

Numer certyfikatu: …….

Data ważności certyfikatu: …….

[ ] Certyfikat Audytora Wewnętrznego normy ISO/IEC 27701 wydany przez akredytowaną jednostkę certyfikującą (wymagany)

Nazwa jednostki certyfikującej: …….

Numer certyfikatu: …….

Data ważności certyfikatu: …….

Audyt powdrożeniowy (Zadanie 4) - osoba przeprowadzająca audyt:

Imię i nazwisko: …….

Posiadany certyfikat:

[ ] Certyfikat Audytora Wiodącego SZBI wg PN-EN ISO/IEC 27001:2022 wydany przez akredytowaną jednostkę certyfikującą (wymagany)

Nazwa jednostki certyfikującej: …….

Numer certyfikatu: …….

Data ważności certyfikatu: …….

Doświadczenie Wykonawcy

(co najmniej 3 audyty bezpieczeństwa informacji lub wdrożeń SZBI w jednostkach administracji publicznej)

1. Nazwa zamawiającego: ……. Zakres zamówienia: ……. Rok realizacji: …….

2. Nazwa zamawiającego: …… Zakres zamówienia: …… Rok realizacji: ……

3. Nazwa zamawiającego: …… Zakres zamówienia: …… Rok realizacji: ……

4. Nazwa zamawiającego: …… Zakres zamówienia: …… Rok realizacji: ……

5. Nazwa zamawiającego: …… Zakres zamówienia: …… Rok realizacji: ……

Uwagi i informacje dodatkowe Wykonawcy: ……

Oświadczenia Wykonawcy

Oświadczenie o znajomości przepisów prawa

Oświadczam, że posiadam znajomość przepisów prawa obowiązujących jednostki samorządu terytorialnego w zakresie bezpieczeństwa informacji, w szczególności:

- Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności (KRI);
- ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (KSC);
- 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 (RODO).

Oświadczenie ogólne

Oświadczam, że zapoznałem/zapoznałam się z treścią zapytania ofertowego i zobowiązuję się do realizacji zamówienia na warunkach w nim określonych, w tym do zakończenia audytu powdrożeniowego nie później niż do dnia 15 września 2026 r. Wyrażam zgodę na udostępnienie dokumentacji związanej z realizacją zamówienia instytucjom uprawnionym do kontroli projektu grantowego “Cyberbezpieczny Samorząd”, realizowanego na podstawie umowy nr FERC.02.02-CS.01.001/23/2399/FERC.02.02-CS.01-001/23/2024.

Miejscowość i data: ……

Podpis i pieczęć Wykonawcy: ……

FORMULARZ OFERTY NR 2

GMINNY OŚRODEK POMOCY SPOŁECZNEJ W CEKOWIE-KOLONII

Zapytanie ofertowe nr USC.EL.271.1.2.2026

DANE WYKONAWCY:

Nazwa firmy / imię i nazwisko: …….

Adres: …….

NIP: …….

REGON: …….

Osoba do kontaktu: …….

Telefon: …….

E-mail: …….

ZAMAWIAJĄCY: Gminny Ośrodek Pomocy Społecznej w Cekowie-Kolonii, Ceków-Kolonia 51, 62-834 Ceków NIP GOPS: 9680770226

TABELA WYCENY

Lp.	Zakres usługi	Cena netto (zł)	Stawka VAT (%)	Cena brutto (zł)
1.	Audyt wstępny (przedwdrożeniowy) - analiza luk, inwentaryzacja aktywów, ocena stanu bezpieczeństwa			
2.	Przegląd aktualnie posiadanych polityk bezpieczeństwa informacji i ocena ich zgodności z obowiązującymi przepisami			
3.	Opracowanie dokumentacji SZBI (polityki, procedury, instrukcje, rejestry) dostosowanej do specyfiki GOPS			
4.	Wdrożenie dokumentacji SZBI (wprowadzenie zarządzeń, wsparcie przy wdrożeniu procedur operacyjnych)			

Lp.	Zakres usługi	Cena netto (zł)	Stawka VAT (%)	Cena brutto (zł)
5.	Audyt powdrożeniowy - weryfikacja wdrożenia, identyfikacja niezgodności, działania korygujące			
	RAZEM			

Infrastruktura objęta zamówieniem (GOPS):

- Korzystanie ze wspólnej infrastruktury serwerowej (2 serwery, system backupu, monitoring, system alarmowy, agregat)
- 7 komputerów stacjonarnych
- 1 laptop
- 4 telefony służbowe z systemem Android

Proponowany harmonogram realizacji:

Audyt wstępny: od …….. do ……..

Przegląd i aktualizacja polityk: od …….. do ……..

Opracowanie dokumentacji SZBI: od …….. do ……..

Wdrożenie dokumentacji SZBI: od …….. do ……..

Audyt powdrożeniowy: od …….. do …….. (nieprzekraczalnie do 15.09.2026 r.)

Łączny termin realizacji zamówienia (w dniach kalendarzowych od dnia podpisania umowy): …….. dni

Informacja dotycząca audytu

Audyt wstępny i powdrożeniowy zostanie przeprowadzony przez: (zaznaczyć właściwe)

[ ] Wykonawcę we własnym zakresie

[ ] Podmiot zewnętrzny działający na zlecenie Wykonawcy

Jeżeli przez podmiot zewnętrzny - nazwa i dane podmiotu:
……

Kwalifikacje i certyfikaty osób przeprowadzających audyt

Audyt wstępny (Zadanie 3) - osoba przeprowadzająca audyt:

Imię i nazwisko: …….

Posiadany certyfikat (zaznaczyć właściwe):

[ ] Certyfikat Audytora Wiodącego SZBI wg PN-EN ISO/IEC 27001:2022 wydany przez akredytowaną jednostkę certyfikującą

[ ] Certyfikat Audytora Wewnętrznego SZBI wg PN-EN ISO/IEC 27001:2022 wydany przez akredytowaną jednostkę certyfikującą

Nazwa jednostki certyfikującej: …….

Numer certyfikatu: …….

Data ważności certyfikatu: …….

[ ] Certyfikat Audytora Wewnętrznego normy ISO/IEC 27701 wydany przez akredytowaną jednostkę certyfikującą (wymagany)

Nazwa jednostki certyfikującej: …….

Numer certyfikatu: …….

Data ważności certyfikatu: …….

Audyt powdrożeniowy (Zadanie 4) - osoba przeprowadzająca audyt:

Imię i nazwisko: …….

Posiadany certyfikat:

[ ] Certyfikat Audytora Wiodącego SZBI wg PN-EN ISO/IEC 27001:2022 wydany przez akredytowaną jednostkę certyfikującą (wymagany)

Nazwa jednostki certyfikującej: …….

Numer certyfikatu: …….

Data ważności certyfikatu: …….

Doświadczenie Wykonawcy

(proszę wskazać co najmniej 3 audyty bezpieczeństwa informacji lub wdrożenia SZBI w jednostkach administracji publicznej)

1. Nazwa zamawiającego: ……. Zakres zamówienia: ……. Rok realizacji: …….
2. Nazwa zamawiającego: ……. Zakres zamówienia: ……. Rok realizacji: …….

3. Nazwa zamawiającego: …… Zakres zamówienia: …… Rok realizacji: …….
4. Nazwa zamawiającego: …… Zakres zamówienia: …… Rok realizacji: …….
5. Nazwa zamawiającego: …… Zakres zamówienia: …… Rok realizacji: …….

Uwagi i informacje dodatkowe Wykonawcy: …….

Oświadczenia Wykonawcy

Oświadczenie o znajomości przepisów prawa

Oświadczam, że posiadam znajomość przepisów prawa obowiązujących jednostki samorządu terytorialnego w zakresie bezpieczeństwa informacji, w szczególności:

- Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności (KRI);
- ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (KSC);
- 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 (RODO).

Oświadczenie ogólne

Oświadczam, że zapoznałem/zapoznałam się z treścią zapytania ofertowego i zobowiązuję się do realizacji zamówienia na warunkach w nim określonych, w tym do zakończenia audytu powdrożeniowego nie później niż do dnia 15 września 2026 r. Wyrażam zgodę na udostępnienie dokumentacji związanej z realizacją zamówienia instytucjom uprawnionym do kontroli projektu grantowego “Cyberbezpieczny Samorząd”, realizowanego na podstawie umowy nr FERC.02.02-CS.01.001/23/2399/FERC.02.02-CS.01-001/23/2024.

Miejscowość i data: …….

Podpis i pieczęć Wykonawcy: …….

FORMULARZ OFERTY NR 3

GMINNE CENTRUM PROMOCJI KULTURY, SPORTU I REKREACJI W CEKOWIE-KOLONII

Zapytanie ofertowe nr USC.EL.271.1.3.2026

DANE WYKONAWCY:

Nazwa firmy / imię i nazwisko: …….

Adres: …….

NIP: …….

REGON: …….

Osoba do kontaktu: …….

Telefon: …….

E-mail: …….

ZAMAWIAJĄCY: Gminne Centrum Promocji Kultury, Sportu i Rekreacji w Cekowie-Kolonii, Ceków-Kolonia 51, 62-834 Ceków NIP GCPKSiR: 9680973834

TABELA WYCENY

Lp.	Zakres usługi	Cena netto (zł)	Stawka VAT (%)	Cena brutto (zł)
1.	Audyt wstępny (przedwdrożeniowy) - analiza luk, inwentaryzacja aktywów, ocena stanu bezpieczeństwa			
2.	Przegląd aktualnie posiadanych polityk bezpieczeństwa informacji i ocena ich zgodności z obowiązującymi przepisami			
3.	Opracowanie dokumentacji SZBI (polityki, procedury, instrukcje, rejestry) dostosowanej do specyfiki GCPKSiR			
4.	Wdrożenie dokumentacji SZBI (wprowadzenie zarządzeń, wsparcie przy wdrożeniu procedur operacyjnych)			

Lp.	Zakres usługi	Cena netto (zł)	Stawka VAT (%)	Cena brutto (zł)
5.	Audyt powdrożeniowy - weryfikacja wdrożenia, identyfikacja niezgodności, działania korygujące			
	RAZEM			

Infrastruktura objęta zamówieniem (GCPKSiR):

- Korzystanie ze wspólnej infrastruktury serwerowej (2 serwery, system backupu, monitoring, system alarmowy, agregat)
- 2 komputery stacjonarne
- 1 telefon służbowy z systemem Android

Proponowany harmonogram realizacji:

Audyt wstępny: od …….. do ……..

Przegląd i aktualizacja polityk: od …….. do ……..

Opracowanie dokumentacji SZBI: od …….. do ……..

Wdrożenie dokumentacji SZBI: od …….. do ……..

Audyt powdrożeniowy: od …….. do …….. (nieprzekraczalnie do 15.09.2026 r.)

Łączny termin realizacji zamówienia (w dniach kalendarzowych od dnia podpisania umowy): …….. dni

Informacja dotycząca audytu

Audyt wstępny i powdrożeniowy zostanie przeprowadzony przez: (zaznaczyć właściwe)

[ ] Wykonawcę we własnym zakresie

[ ] Podmiot zewnętrzny działający na zlecenie Wykonawcy

Jeżeli przez podmiot zewnętrzny - nazwa i dane podmiotu:
……

Kwalifikacje i certyfikaty osób przeprowadzających audyt

Audyt wstępny (Zadanie 3) - osoba przeprowadzająca audyt:

Imię i nazwisko: …….

Posiadany certyfikat (zaznaczyć właściwe):

[ ] Certyfikat Audytora Wiodącego SZBI wg PN-EN ISO/IEC 27001:2022 wydany przez akredytowaną jednostkę certyfikującą

[ ] Certyfikat Audytora Wewnętrznego SZBI wg PN-EN ISO/IEC 27001:2022 wydany przez akredytowaną jednostkę certyfikującą

Nazwa jednostki certyfikującej: …….

Numer certyfikatu: …….

Data ważności certyfikatu: …….

[ ] Certyfikat Audytora Wewnętrznego normy ISO/IEC 27701 wydany przez akredytowaną jednostkę certyfikującą (wymagany)

Nazwa jednostki certyfikującej: …….

Numer certyfikatu: …….

Data ważności certyfikatu: …….

Audyt powdrożeniowy (Zadanie 4) - osoba przeprowadzająca audyt:

Imię i nazwisko: …….

Posiadany certyfikat:

[ ] Certyfikat Audytora Wiodącego SZBI wg PN-EN ISO/IEC 27001:2022 wydany przez akredytowaną jednostkę certyfikującą (wymagany)

Nazwa jednostki certyfikującej: …….

Numer certyfikatu: …….

Data ważności certyfikatu: …….

Doświadczenie Wykonawcy

proszę wskazać co najmniej 3 audyty bezpieczeństwa informacji lub wdrożenia SZBI w jednostkach administracji publicznej)

1. Nazwa zamawiającego: ……. Zakres zamówienia: ……. Rok realizacji: …….
2. Nazwa zamawiającego: ……. Zakres zamówienia: ……. Rok realizacji: …….
3. Nazwa zamawiającego: ……. Zakres zamówienia: ……. Rok realizacji: …….

4. Nazwa zamawiającego: …… Zakres zamówienia: …… Rok realizacji: …….
5. Nazwa zamawiającego: …… Zakres zamówienia: …… Rok realizacji: …….

Uwagi i informacje dodatkowe Wykonawcy: …….

Oświadczenia Wykonawcy

Oświadczenie o znajomości przepisów prawa

Oświadczam, że posiadam znajomość przepisów prawa obowiązujących jednostki samorządu terytorialnego w zakresie bezpieczeństwa informacji, w szczególności:

- Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności (KRI);
- ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (KSC);
- 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 (RODO).

Oświadczenie ogólne

Oświadczam, że zapoznałem/zapoznałam się z treścią zapytania ofertowego i zobowiązuję się do realizacji zamówienia na warunkach w nim określonych, w tym do zakończenia audytu powdrożeniowego nie później niż do dnia 15 września 2026 r. Wyrażam zgodę na udostępnienie dokumentacji związanej z realizacją zamówienia instytucjom uprawnionym do kontroli projektu grantowego “Cyberbezpieczny Samorząd”, realizowanego na podstawie umowy nr FERC.02.02-CS.01.001/23/2399/FERC.02.02-CS.01-001/23/2024.

Miejscowość i data: …….

Podpis i pieczęć Wykonawcy: …….

FORMULARZ OFERTY NR 4

GMINNY ZESPÓŁ OBSŁUGI ADMINISTRACYJNEJ I EKONOMICZNEJ OŚWIATY W CEKOWIE-KOLONII

Zapytanie ofertowe nr USC.EL.271.1.4.2026

DANE WYKONAWCY:

Nazwa firmy / imię i nazwisko: …….

Adres: …….

NIP: …….

REGON: …….

Osoba do kontaktu: …….

Telefon: …….

E-mail: …….

ZAMAWIAJĄCY: Gminny Zespół Obsługi Administracyjnej i Ekonomicznej Oświaty w Cekowie-Kolonii, Ceków-Kolonia 51, 62-834 Ceków NIP GZOAEO: 9680000451

TABELA WYCENY

Lp.	Zakres usługi	Cena netto (zł)	Stawka VAT (%)	Cena brutto (zł)
1.	Audyt wstępny (przedwdrożeniowy) - analiza luk, inwentaryzacja aktywów, ocena stanu bezpieczeństwa			
2.	Przegląd aktualnie posiadanych polityk bezpieczeństwa informacji i ocena ich zgodności z obowiązującymi przepisami			
3.	Opracowanie dokumentacji SZBI (polityki, procedury, instrukcje, rejestry) dostosowanej do specyfiki GZOAEO			
4.	Wdrożenie dokumentacji SZBI (wprowadzenie zarządzeń, wsparcie przy wdrożeniu procedur operacyjnych)			

Lp.	Zakres usługi	Cena netto (zł)	Stawka VAT (%)	Cena brutto (zł)
5.	Audyt powdrożeniowy - weryfikacja wdrożenia, identyfikacja niezgodności, działania korygujące			
	RAZEM			

Infrastruktura objęta zamówieniem (GZOAEO):

- Korzystanie ze wspólnej infrastruktury serwerowej (2 serwery, system backupu, monitoring, system alarmowy, agregat)
- 4 komputery stacjonarne
- 1 telefon służbowy z systemem Android

Proponowany harmonogram realizacji:

Audyt wstępny: od …….. do ……..

Przegląd i aktualizacja polityk: od …….. do ……..

Opracowanie dokumentacji SZBI: od …….. do ……..

Wdrożenie dokumentacji SZBI: od …….. do ……..

Audyt powdrożeniowy: od …….. do …….. (nieprzekraczalnie do 15.09.2026 r.)

Łączny termin realizacji zamówienia (w dniach kalendarzowych od dnia podpisania umowy): …….. dni

Informacja dotycząca audytu

Audyt wstępny i powdrożeniowy zostanie przeprowadzony przez: (zaznaczyć właściwe)

[ ] Wykonawcę we własnym zakresie

[ ] Podmiot zewnętrzny działający na zlecenie Wykonawcy

Jeżeli przez podmiot zewnętrzny - nazwa i dane podmiotu:
……

Kwalifikacje i certyfikaty osób przeprowadzających audyt

Audyt wstępny (Zadanie 3) - osoba przeprowadzająca audyt:

Imię i nazwisko: …….

Posiadany certyfikat (zaznaczyć właściwe):

Imię i nazwisko: …….

Posiadany certyfikat (zaznaczyć właściwe):

[ ] Certyfikat Audytora Wiodącego SZBI wg PN-EN ISO/IEC 27001:2022 wydany przez akredytowaną jednostkę certyfikującą

[ ] Certyfikat Audytora Wewnętrznego SZBI wg PN-EN ISO/IEC 27001:2022 wydany przez akredytowaną jednostkę certyfikującą

Nazwa jednostki certyfikującej: …….

Numer certyfikatu: …….

Data ważności certyfikatu: …….

[ ] Certyfikat Audytora Wewnętrznego normy ISO/IEC 27701 wydany przez akredytowaną jednostkę certyfikującą (wymagany)

Nazwa jednostki certyfikującej: …….

Numer certyfikatu: …….

Data ważności certyfikatu: …….

Audyt powdrożeniowy (Zadanie 4) - osoba przeprowadzająca audyt:

Imię i nazwisko: …….

Posiadany certyfikat:

[ ] Certyfikat Audytora Wiodącego SZBI wg PN-EN ISO/IEC 27001:2022 wydany przez akredytowaną jednostkę certyfikującą (wymagany)

Nazwa jednostki certyfikującej: …….

Numer certyfikatu: …….

Data ważności certyfikatu: …….

Doświadczenie Wykonawcy

(proszę wskazać co najmniej 3 audyty bezpieczeństwa informacji lub wdrożenia SZBI w jednostkach administracji publicznej)

1. Nazwa zamawiającego: ……. Zakres zamówienia: ……. Rok realizacji: …….
2. Nazwa zamawiającego: ……. Zakres zamówienia: ……. Rok realizacji: …….

3. Nazwa zamawiającego: …… Zakres zamówienia: …… Rok realizacji: ……
4. Nazwa zamawiającego: …… Zakres zamówienia: …… Rok realizacji: ……
5. Nazwa zamawiającego: …… Zakres zamówienia: …… Rok realizacji: ……

Uwagi i informacje dodatkowe Wykonawcy: ……

Oświadczenia Wykonawcy

Oświadczenie o znajomości przepisów prawa

Oświadczam, że posiadam znajomość przepisów prawa obowiązujących jednostki samorządu terytorialnego w zakresie bezpieczeństwa informacji, w szczególności:

- Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności (KRI);
- ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (KSC);
- 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 (RODO).

Oświadczenie ogólne

Oświadczam, że zapoznałem/zapoznałam się z treścią zapytania ofertowego i zobowiązuję się do realizacji zamówienia na warunkach w nim określonych, w tym do zakończenia audytu powdrożeniowego nie później niż do dnia 15 września 2026 r. Wyrażam zgodę na udostępnienie dokumentacji związanej z realizacją zamówienia instytucjom uprawnionym do kontroli projektu grantowego “Cyberbezpieczny Samorząd”, realizowanego na podstawie umowy nr FERC.02.02-CS.01.001/23/2399/FERC.02.02-CS.01-001/23/2024.

Miejscowość i data: ……

Podpis i pieczęć Wykonawcy: ……