

Kaczory, dnia 24 lutego 2026 r.

ZP.272.2.2026

ZAPYTANIE OFERTOWE dotyczy SZBI w ramach projektu „Cyberbezpieczny samorząd”.
Wartość szacunkowa poniżej 170 000 złotych netto.

Burmistrz Miasta i Gminy Kaczory, zaprasza do składania ofert na zadanie pn.

**Opracowanie, ustanowienie i wdrożenie Systemu Zarządzania Bezpieczeństwem
Informacji (SZBI) w ramach projektu „Cyberbezpieczny Samorząd” dla 4 jednostek
organizacyjnych Miasta i Gminy Kaczory**

Zamawiający:

MIASTO I GMINA KACZORY

ul. Piłska 1

64 – 810 Kaczory

tel. (67) 284 23 71

działając na podstawie art. 2 ust. 1 pkt 1 ustawy z dnia 11 września 2019 r. Prawo zamówień
publicznych

(Dz. U. z 2024r., poz. 1320 ze zm.)

Zadanie stanowiące przedmiot niniejszego postępowania realizowane jest w ramach projektu pn.: „Cyberbezpieczny samorząd” realizowanego z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa, w ramach Projektu grantowego „Cyberbezpieczny samorząd”, Umowa o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/0492/FERC.02.02-CS.01-001/23/2024.

1. Podstawa i cel zamówienia

1. Zamówienie realizowane w związku z projektem grantowym „Cyberbezpieczny Samorząd” (FERC 2021–2027, Priorytet II, Działanie 2.2 – Wzmocnienie krajowego systemu cyberbezpieczeństwa).
2. Celem zamówienia jest opracowanie, ustanowienie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w Urzędzie Miasta i Gminy w Kaczorach (UMiG), Zakładzie Usług Wodnych i Kanalizacyjnych w Kaczorach (ZUWiK), Miejsko-Gminnym Zespole Oświaty w Kaczorach (MGZO) oraz Miejsko-Gminnym Ośrodku Pomocy Społecznej w Kaczorach (MGOPS). – zgodnego z wymaganiami:

- o aktualnie obowiązującego Rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności (KRI),
- o normy PN-EN ISO/IEC 27001,
- o Ustawy z dnia 5.07.2018 r. o krajowym systemie cyberbezpieczeństwa (UoKSC).

2. Podział kosztów

Wykonawca w formularzu ofertowym podaje ceny w podziale na poszczególne jednostki organizacyjne zgodnie z poniższą tabelą.

Poz.	Jednostka	Zakres
1	UMiG	Opracowanie, ustanowienie i wdrożenie SZBI
2	MGZO	Opracowanie, ustanowienie i wdrożenie SZBI
3	ZUWiK	Opracowanie, ustanowienie i wdrożenie SZBI
4	MGOPS	Opracowanie, ustanowienie i wdrożenie SZBI

3. Zakres przedmiotu zamówienia

W ramach zamówienia Wykonawca zrealizuje następujące prace dla każdej z 4 jednostek:

3.1. Inwentaryzacja i analiza stanu obecnego

1. Przegląd istniejącej dokumentacji.
2. Inwentaryzacja aktywów informacyjnych (systemy teleinformatyczne, rejestry, zbiory danych, nośniki, lokalizacje przetwarzania) we wszystkich jednostkach.
3. Identyfikacja procesów przetwarzania informacji i powiązanych ról.
4. Rozpoznanie istniejących zabezpieczeń technicznych i organizacyjnych.

3.2. Analiza ryzyka

1. Opracowanie lub dostosowanie metodyki analizy ryzyka zgodnej z wymaganiami KRI i normą ISO/IEC 27005 (lub równoważną).
2. Identyfikacja zagrożeń, podatności i skutków dla aktywów informacyjnych.
3. Szacowanie i ocena ryzyka dla każdej jednostki.
4. Opracowanie planu postępowania z ryzykiem z przypisaniem odpowiedzialności.
5. Przedstawienie wyników analizy ryzyka kierownictwu Zamawiającego i uzyskanie akceptacji poziomu ryzyka szacunkowego.

3.3. Opracowanie dokumentacji SZBI

Wykonawca opracuje kompletny zestaw dokumentacji SZBI, obejmujący co najmniej:

1. **Politykę Bezpieczeństwa Informacji (PBI)** – nadrzędny dokument określający cele, zakres i zasady bezpieczeństwa informacji.
2. **Zakres SZBI** – określenie granic systemu (jednostki, procesy, lokalizacje, systemy teleinformatyczne).
3. **Deklarację stosowania (SoA)** – wykaz zabezpieczeń z Załącznika A normy ISO/IEC 27001.
4. **Procedury i instrukcje operacyjne**, w tym co najmniej:
 - procedura zarządzania incydentami bezpieczeństwa informacji,
 - procedura zarządzania dostępem i uprawnieniami,
 - procedura zarządzania kopiami zapasowymi,
 - procedura zarządzania zmianami w systemach teleinformatycznych,
 - procedura zarządzania nośnikami i informacją w formie papierowej,
 - procedura bezpiecznej pracy zdalnej,
 - procedura postępowania z naruszeniami ochrony danych osobowych (powiązana z RODO),
 - instrukcja zarządzania systemem teleinformatycznym (w rozumieniu KRI).
5. **Plan ciągłości działania (BCP)** i podstawowe założenia planu odtwarzania po awarii (DRP).
6. **Klasyfikacja informacji** – zasady klasyfikowania, oznaczania i postępowania z informacjami.
7. **Wzory dokumentów operacyjnych**: rejestr incydentów, rejestr aktywów, formularz upoważnienia do przetwarzania, oświadczenie o poufności, karta przeglądu SZBI.
8. **Instrukcja samodzielnej aktualizacji SZBI** (1–2 strony) – opisująca kiedy i jak Zamawiający powinien dokonywać przeglądów i aktualizacji dokumentacji SZBI, w tym: aktualizacji analizy ryzyka, dodawania nowych systemów, modyfikacji procedur, harmonogramu przeglądów.

3.4. Wdrożenie SZBI

1. Prezentacja dokumentacji SZBI kierownictwu Zamawiającego i uzyskanie formalnego zatwierdzenia.
2. Przekazanie dokumentacji w formie edytowalnej (.docx lub równoważny) oraz w formacie PDF.
3. Przeprowadzenie warsztatu wdrożeniowego dla osób kluczowych (kierownictwo, IOD, IT) – min. 2 godziny na każdą jednostkę (łącznie min. 8 godzin). Warsztat obejmie omówienie struktury dokumentacji, obowiązków i sposobu stosowania procedur w praktyce.
4. Wsparcie przy wydaniu zarządzeń wewnętrznych wprowadzających SZBI w jednostkach.

4. Wymagania dotyczące dokumentacji

1. Dokumentacja musi być zgodna z wymaganiami aktualnie obowiązującego rozporządzenia w sprawie KRI, normą PN-EN ISO/IEC 27001 oraz przepisami o ochronie danych osobowych (RODO).
2. Dokumentacja musi uwzględniać systemy teleinformatyczne nowo zakupione w ramach projektu „Cyberbezpieczny Samorząd”.
3. Dokumentacja musi być napisana prostym, zrozumiałym językiem – adresatami są pracownicy urzędu i jednostek, nie specjaliści IT. Terminy techniczne powinny być objaśnione lub zdefiniowane w słowniku.
4. Dokumentacja musi mieć strukturę modułową umożliwiającą samodzielną aktualizację przez Zamawiającego.
5. Wykonawca prześle dokumentację w formacie edytowalnym (.docx lub równoważny) oraz PDF.

6. Zamawiający nabywa niewyłączną, nieograniczoną terytorialnie i czasowo licencję na wykorzystywanie, kopiowanie, modyfikowanie i udostępnianie wewnętrzne otrzymanej dokumentacji SZBI bez dodatkowych opłat.

5. Termin realizacji

Wykonawca zrealizuje całość zamówienia w terminie **do 30 dni kalendarzowych od dnia zawarcia umowy**.

Za dzień zakończenia realizacji uznaje się dzień podpisania przez obie strony protokołu odbioru końcowego.

6. Rezultaty i produkty zamówienia

1. Dokument analizy ryzyka z planem postępowania z ryzykiem.
2. Kompletna dokumentacja SZBI (PBI, zakres SZBI, SoA, procedury, instrukcje, BCP/DRP, klasyfikacja informacji, wzory dokumentów) – w formie edytowalnej i PDF.
3. Instrukcja samodzielnej aktualizacji SZBI przez Zamawiającego.
4. Protokół z warsztatu wdrożeniowego z listą obecności.
5. Zarządzenia wewnętrzne wprowadzające SZBI w jednostkach (przygotowane z udziałem Wykonawcy).

7. Kryteria odbioru

Warunki odbioru końcowego:

1. Przekazanie dokumentu analizy ryzyka z planem postępowania z ryzykiem, zaakceptowanego przez kierownictwo Zamawiającego.
2. Przekazanie kompletnej dokumentacji SZBI zgodnej z wymaganiami KRI i normą ISO/IEC 27001, w formacie edytowalnym i PDF, zaakceptowanej przez Zamawiającego.
3. Przekazanie instrukcji samodzielnej aktualizacji SZBI.
4. Przeprowadzenie warsztatu wdrożeniowego dla kadry zarządczej (min. 2h na jednostkę) i przekazanie protokołu z listą obecności.
5. Formalne wprowadzenie SZBI w jednostkach (wydanie zarządzeń wewnętrznych z udziałem Wykonawcy).
6. Dokumentacja napisana zrozumiałym językiem, ma strukturę modułową i umożliwia samodzielną aktualizację.

Zamawiający ma 5 dni roboczych na zgłoszenie uwag do przekazanych produktów. Wykonawca wprowadzi uzgodnione poprawki w ciągu 3 dni roboczych od otrzymania uwag, w ramach wynagrodzenia umownego.

8. Wymogi organizacyjne

8.1. Współpraca z Zamawiającym

Zamawiający wyznaczy koordynatora projektu po swojej stronie. Wykonawca będzie współpracować z koordynatorem, kierownictwem jednostek, inspektorem ochrony danych (IOD) oraz zespołem IT.

8.2. Forma realizacji

Dopuszcza się realizację mieszaną: wizyty w siedzibach jednostek (inventaryzacja, wywiady, warsztat wdrożeniowy) oraz praca zdalna (opracowanie dokumentacji). Warsztat wdrożeniowy odbędzie się stacjonarnie.

8.3. Oznaczenia projektu

Wszystkie dokumenty wytworzone w ramach zamówienia oznaczone zgodnie z wytycznymi FERC/UE, z informacją o współfinansowaniu.

8.4. Poufność

Wykonawca i wszystkie osoby zaangażowane w realizację złożą oświadczenia o zachowaniu poufności. Wykonawca nie będzie wykorzystywał informacji uzyskanych od Zamawiającego do celów innych niż realizacja niniejszego zamówienia.

8.5. Bezpieczeństwo informacji

Wykonawca zobowiązuje się do niewykorzystywania publicznych usług AI w sposób prowadzący do ujawnienia danych Zamawiającego bez odrębnej zgody Zamawiającego.

9. Wymagania wobec Wykonawcy

9.1. Doświadczenie

Wykonawca musi wykazać, że w okresie ostatnich 3 lat przed terminem składania ofert zrealizował co najmniej 2 usługi obejmujące opracowanie i wdrożenie SZBI (w tym analizę ryzyka i dokumentację) dla podmiotów publicznych, o wartości co najmniej 5 000 PLN brutto każda. Mile widziane doświadczenie w pracy z jednostkami samorządu terytorialnego.

9.2. Personel

Wykonawca zapewni co najmniej jedną osobę kluczową (konsultanta wiodącego), która spełnia łącznie następujące wymagania:

- posiada certyfikat typu ISO/IEC 27001 Lead Implementer lub Lead Auditor (lub równoważny),
- posiada doświadczenie min. 2 lata w opracowywaniu i wdrażaniu SZBI,
- w ciągu ostatnich 3 lat uczestniczyła w co najmniej 2 projektach wdrożenia SZBI dla podmiotów publicznych.

9.3. Informacje wymagane z ofertą

Wraz z ofertą Wykonawca przedstawi:

- wykaz zrealizowanych usług potwierdzających spełnienie warunku z pkt 9.1,
- kopię certyfikatu konsultanta wiodącego (pkt 9.2),
- krótkie CV konsultanta wiodącego (z opisem doświadczenia w projektach SZBI dla sektora publicznego).

10. Kryterium oceny ofert

1. Zamawiający dokona oceny ofert na podstawie jednego kryterium:

Kryterium	Waga	Maks. punktów
Cena brutto	100%	100

$$\text{Wzór: } C = (C_{\min} / C_{\text{badana}}) \times 100$$

gdzie: C_{\min} – najniższa cena brutto spośród ofert niepodlegających odrzuceniu; C_{badana} – cena brutto oferty badanej.

2. Wybrana zostanie najkorzystniejsza oferta zawierająca najniższą cenę (jako cenę należy rozumieć kwotę brutto za wykonanie w całości zamówienie) oraz spełni wszystkie wymagania określone w niniejszym OPZ.

3. Cena podana w ofercie powinna zawierać wszelkie koszty i składniki związane z wykonaniem zamówienia, uwzględniając cały zakres przedmiotu zamówienia. W cenie należy przewidzieć ewentualne koszty, które mogą wynikać w trakcie realizacji zadania a będą niezbędne do jego prawidłowego wykonania.

4. Jeżeli nie można dokonać wyboru oferty najkorzystniejszej ze względu na to, że zostały złożone oferty o takiej samej cenie, Zamawiający wezwie Wykonawców, którzy złożyli te oferty, do złożenia w terminie wyznaczonym przez Zamawiającego ofert dodatkowych. Wykonawcy nie mogą zaoferować cen wyższych niż zaoferowane w złożonych ofertach.

11. Zasady rozliczeń

1. Cena ofertowa obejmuje całość kosztów związanych z realizacją zamówienia: inwentaryzację, analizę ryzyka, opracowanie dokumentacji, warsztat wdrożeniowy, ewentualne poprawki dokumentacji.
2. Wykonawca wyodrębni na fakturze pozycje umożliwiające przypisanie kosztów do poszczególnych jednostek organizacyjnych zgodnie z tabelą w rozdziale 2.
3. Zamawiający informuje, że zamówienie jest finansowane w ponad 70% ze środków publicznych. Usługi doradcze mogą podlegać zwolnieniu z VAT. Wykonawca zobowiązany jest do prawidłowego określenia stawki VAT w ofercie.

12. CPV (Słownik zamówień)

- 79417000-0 – Usługi doradcze w zakresie bezpieczeństwa
- 72220000-3 – Usługi doradcze w zakresie systemów i doradztwo techniczne

13. Postanowienia dot. ochrony danych i informacji

1. Wykonawca zapewni zgodność przetwarzania danych osobowych z przepisami RODO; w razie potrzeby zawarta zostanie umowa powierzenia przetwarzania danych.
2. Wykonawca zobowiązuje się do ochrony wszelkich informacji uzyskanych w toku realizacji zamówienia.

14. Dostępność i równość szans

1. Dokumentacja SZBI będzie przygotowana w sposób umożliwiający powiększanie treści i wydruk w dobrej jakości, z zachowaniem odpowiedniego kontrastu i czytelnych czcionek.
2. Realizacja zamówienia odbywa się z poszanowaniem zasady równości szans kobiet i mężczyzn oraz niedyskryminacji.
3. Realizacja zamówienia będzie zgodna ze „Standardami dostępności dla polityki spójności 2021-2027”.

15. Informacje końcowe

1. W sprawach nieuregulowanych niniejszym OPZ zastosowanie mają właściwe przepisy oraz wytyczne konkursu „Cyberbezpieczny Samorząd”.
2. Złożenie oferty jest równoznaczne z akceptacją treści niniejszego OPZ.
3. Wykonawca niniejszego zamówienia nie może być jednocześnie wykonawcą audytów zgodności z KRI realizowanych w ramach tego samego projektu grantowego.
4. Niniejsze zapytanie ofertowe nie stanowi zobowiązania Miasta i Gminy Kaczory do zawarcia umowy.
5. Miasto i Gmina Kaczory zastrzega sobie prawo do unieważnienia postępowania bez podania przyczyny.

16. Miejsce i termin składania ofert

Ofertę należy złożyć do dnia 11 marca 2026 r. do godziny 15.00.

Otwarcie ofert nastąpi w dniu 11 marca 2026 r. o godz. 15.15.

Ofertę należy złożyć wyłącznie za pośrednictwem Bazy Konkurencyjności pod adresem <https://bazakonkurencyjnosci.funduszeuropejskie.gov.pl/ogloszenia/266263>

17. Kontakt

Dodatkowe informacje dotyczące zamówienia można uzyskać:

1. W sprawach merytorycznych u p. Mateusza Grzesiuka tel. 663 222 820
2. W sprawach zamówienia publicznego u p. Kariny Jaśniak tel. 663 222 172