

Kaczory, dnia 16 lutego 2026 r.

ZP.272.1.2026

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

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

„Usługa szkoleniowa w ramach projektu „Cyberbezpieczny Samorząd” – szkolenia z bezpieczeństwa informacji i cyberbezpieczeństwa dla wszystkich pracowników oraz szkolenia dedykowane dla kadry kierowniczej i informatyków w obszarze wdrożenia SZBI”

Zamawiający:

MIASTO I GMINA KACZORY

ul. Pilska 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.)

I Opis przedmiotu zamówienia:

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 podniesienie kompetencji pracowników Zamawiającego w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa oraz przygotowanie kadry kierowniczej i zespołu IT do wdrażania, utrzymania i doskonalenia Systemu Zarządzania Bezpieczeństwem

Informacji (SZBI) zgodnego z wymaganiami KRI (rozporządzenie z 21.05.2024 r.) i normą PN-EN ISO/IEC 27001.

3. Szkolenia obejmują podstawowe wiadomości z bezpieczeństwa informacji i ochrony danych osobowych, z uwzględnieniem regulacji wewnętrznych Zamawiającego (polityki, procedury) oraz wymagań KRI; kładą nacisk na praktyczne stosowanie procedur i narzędzi SZBI w codziennej pracy.
4. Szkolenia są dostępne dla wszystkich pracowników Urzędu Miasta i Gminy w Kaczorach (UMiG) oraz jednostek organizacyjnych Zamawiającego tj. Zakład Usług Wodnych i Kanalizacyjnych w Kaczorach (ZUWiK), Miejsko-Gminny Zespół Oświaty w Kaczorach (MGZO); Miejsko-Gminny Ośrodek Pomocy Społecznej w Kaczorach (MGOPS).

2. Zakres rzeczowy zamówienia

- Łączna liczba unikalnych pracowników: 74.
- Każdy pracownik uczestniczy w zadaniach A i B (stacjonarnie lub ścieżka uzupełniająca).
- 9 osób z kadry kierowniczej (poz. 9, 11–13) uczestniczy dodatkowo w zadaniu C.
- 2 informatyków (poz. 10) uczestniczy dodatkowo w zadaniu D. Zespół IT obsługuje wszystkie cztery jednostki, ale budżetowo jest przypisany do UMiG.

Poz.	Jednostka	Zadanie OPZ	Razem	Uwagi
1	UMiG	A – bezpieczeństwo informacji	52	wszyscy pracownicy UMiG
2	MGZO	A – bezpieczeństwo informacji	6	
3	ZUWiK	A – bezpieczeństwo informacji	10	
4	MGOPS	A – bezpieczeństwo informacji	6	
	Suma zadanie A		74	
5	UMiG	B – cyberbezpieczeństwo z pokazami	52	ci sami pracownicy co poz. 1
6	MGZO	B – cyberbezpieczeństwo z pokazami	6	ci sami co poz. 2

Poz.	Jednostka	Zadanie OPZ	Razem	Uwagi
7	ZUWiK	B – cyberbezpieczeństwo z pokazami	10	ci sami co poz. 3
8	MGOPS	B – cyberbezpieczeństwo z pokazami	6	ci sami co poz. 4
	Suma zadanie B		74	
9	UMiG	C – kadra kierownicza	5	kadra kier. UMiG (wliczona w poz. 1/5)
10	UMiG	D – zespół IT	2	IT obsługuje wszystkie jednostki (wliczeni w poz. 1/5)
11	MGZO	C – kadra kierownicza	1	kadra kier. MGZO (wliczona w poz. 2/6)
12	ZUWiK	C – kadra kierownicza	2	kadra kier. ZUWiK (wliczona w poz. 3/7)
13	MGOPS	C – kadra kierownicza	1	kadra kier. MGOPS (wliczona w poz. 4/8)
	Suma zadanie C (kadra kier.)		9	wliczeni w zadania A i B
	Suma zadanie D (IT)		2	wliczeni w zadania A i B

Dodatkowe wskaźniki projektu (informacyjnie):

- Liczba systemów służących zwiększeniu poziomu bezpieczeństwa informacji: 7 szt.
- Liczba podmiotów wspartych w zakresie cyberbezpieczeństwa w ramach JST: 3 szt.
- Liczba JST wspartych w zakresie cyberbezpieczeństwa: 1 szt.

Wykonawca w formularzu ofertowym (Załącznik nr 1 do zapytania ofertowego) podaje ceny w podziale na pozycje 1–13 zgodnie z powyższą tabelą. Podział cenowy w ofercie stanowi podstawę do fakturowania i rozliczenia projektu grantowego.

3. Zakres przedmiotowy – zadania

Uwaga dot. modelu realizacji (dla wszystkich pracowników): Zamawiający dopuszcza połączenie treści zadań A i B w jeden dzień szkoleniowy na grupę (tryb stacjonarny). Materiały szkoleniowe w formie PDF służą utrwaleniu i pogłębieniu wiedzy; obowiązkowe zapoznanie się z materiałami dotyczy wyłącznie osób nieobecnych na szkoleniu stacjonarnym oraz nowo zatrudnionych (ścieżka uzupełniająca, patrz pkt 6.3).

Na potrzeby niniejszego OPZ przyjmuje się, że 1 dzień szkoleniowy obejmuje co najmniej 7 godzin dydaktycznych (bez przerw).

4. Liczba uczestników i grupy szkoleniowe

1. Łączna liczba pracowników przewidzianych do przeszkolenia (zadania A i B): **74 osoby**.
2. Kadra kierownicza (zadanie C): **9 osób** – wliczona w pkt 1.
3. Informatycy / zespół IT (zadanie D): **2 osoby** – wliczone w pkt 1.
4. Maksymalna liczebność grup:
 - o zadania A i B: do 25 osób w grupie,
 - o zadanie C: do 9 osób w grupie,
 - o zadanie D: do 2 osób.

5. Wymagania merytoryczne – program szkoleń

Cel ogólny części szkoleniowej: Wzrost świadomości wszystkich pracowników w obszarze przetwarzania informacji oraz praktycznej znajomości regulacji wewnętrznych i wymagań KRI, a także podniesienie kompetencji kadry zarządzającej i IT w zakresie SZBI, analizy ryzyka oraz bezpiecznej konfiguracji systemów teleinformatycznych.

Po zakończeniu cyklu szkoleń zakłada się, że:

- wszyscy pracownicy rozumieją podstawy bezpieczeństwa informacji i ochrony danych osobowych, znają główne cyberzagrożenia i wiedzą, jak stosować procedury SZBI w pracy;
- kadra zarządzająca rozumie SZBI jako narzędzie zapewniania ochrony informacji oraz potrafi nadzorować analizę ryzyka i najważniejsze decyzje bezpieczeństwa;
- kadra IT potrafi bezpiecznie konfigurować i wykorzystywać funkcjonalności bezpieczeństwa w nowo zakupionych i istniejących systemach oraz prowadzić monitoring i reagowanie na incydenty.

Klauzula elastyczności: Szczegółowy zakres tematyczny poszczególnych zadań może zostać doprecyzowany po analizie potrzeb (pkt 6.1), przy zachowaniu celów szkoleniowych określonych w niniejszym rozdziale oraz zgodności z koncepcją projektu grantowego. Zmiana zakresu wymaga pisemnej akceptacji Zamawiającego.

5.1. Zadanie A – Bezpieczeństwo informacji (wszyscy pracownicy)

Cel: ujednolicenie wiedzy o ochronie informacji (w tym danych osobowych), obowiązkach pracowników oraz dobrych praktykach cyberhigieny.

Zakres (poziom świadomości, bez treści konfiguracyjnych IT):

1. **Podstawy bezpieczeństwa informacji** – Poufność–integralność–dostępność; klasyfikacja informacji; oznaczanie i zasady obchodzenia się z informacją jawną, wrażliwą i danymi osobowymi; odpowiedzialność pracownika.
2. **Ochrona danych osobowych w praktyce urzędu** – Role i obowiązki (administrator danych, inspektor ochrony danych, pracownik); najczęstsze błędy i naruszenia oraz ich zgłaszanie (w szczególności procedura 72-godzinna); minimalizacja danych, retencja, upoważnienia, obowiązki zachowania poufności.
3. **Cyberhigiena na stanowisku pracy** – Hasła i frazy hasłowe, korzystanie z menedżerów haseł; uwierzytelnianie wieloskładnikowe (logowanie dwuetapowe); bezpieczny e-mail i przeglądanie stron; praca zdalna i mobilna; zasada „czystego biurka/ekranu”; bezpieczne korzystanie z nośników zewnętrznych.
4. **Socjotechnika** – Typowe techniki manipulacji (pilność, autorytet, ciekawość, strach); sygnały ostrzegawcze w rozmowach telefonicznych, mailach i komunikatorach; proste scenki i ćwiczenia (np. „telefon z banku”, „telefon od przełożonego”).
5. **Zasady korzystania z systemów teleinformatycznych Zamawiającego** – Omówienie kluczowych zapisów regulacji wewnętrznych (polityk, instrukcji, SZBI), w szczególności: instalowanie oprogramowania, korzystanie z poczty prywatnej, przechowywanie dokumentów, praca na danych na urządzeniach prywatnych.
6. **Chmura i współdzielenie plików** – Bezpieczne współdzielenie dokumentów w środowisku chmurowym używanym przez Zamawiającego (uprawnienia, linki publiczne, udostępnienia zewnętrzne) z perspektywy użytkownika.
7. **Bezpieczne korzystanie z narzędzi AI w pracy urzędnika** – Co wolno / czego nie wolno w kontekście SZBI i ochrony danych; zasada niewprowadzania danych osobowych i informacji wrażliwych do publicznych usług AI; przykłady bezpiecznych i niebezpiecznych poleceń; różnica między usługami ogólnodostępnymi a rozwiązaniami wewnętrznymi.
8. **Reagowanie na incydenty** – Jak rozpoznać potencjalny incydent (np. podejrzany e-mail, utrata nośnika, wysłanie maila do niewłaściwego adresata), jak go zgłosić, czego nie robić (np. samodzielne „analizowanie” podejrzanych załączników).
9. **Ćwiczenia / quiz** – Krótki test jednokrotnego wyboru i zadania sytuacyjne (min. 10 pytań) oparte na typowych sytuacjach urzędowych, w tym przykład naruszenia ochrony danych.

Forma i metody: wykład interaktywny z przykładami, dyskusja, ćwiczenia sytuacyjne, krótki test wiedzy (quiz elektroniczny lub papierowy).

Czas trwania:

- wariant rozdzielnny – min. 4 godz. dydaktyczne na grupę,
- wariant 1-dniowy (A+B łącznie) – realizacja efektów uczenia zadania A w ramach co najmniej 7 godzin łącznego czasu dnia.

5.2. Zadanie B – Cyberbezpieczeństwo z pokazami ataków (wszyscy pracownicy)

Cel: zwiększenie świadomości realnych zagrożeń poprzez kontrolowane demonstracje ataków w środowisku testowym (laboratorium Wykonawcy) oraz omówienie prostych, praktycznych mechanizmów ochronnych dostępnych z perspektywy użytkownika.

Pokazy / demonstracje (w środowisku odizolowanym od infrastruktury Zamawiającego):

1. **Phishing i spear-phishing** – Budowa wiadomości phishingowej, domeny łudząco podobne; typowe cechy podejrzanych maili; zasady bezpiecznego postępowania (nieklikanie, zgłaszanie, weryfikacja na drugim kanale).
2. **Ransomware (oprogramowanie wymuszające okup)** – Przykładowy przebieg infekcji (sposób wejścia → szyfrowanie danych); skutki ataku; znaczenie kopii zapasowych; omówienie tego, co pracownik może zrobić, aby ograniczyć skutki (szybkie zgłoszenie, odłączenie sprzętu, niepodejmowanie samodzielnych prób „naprawy”).
3. **Ataki na tożsamość i hasła** – Wykorzystanie skradzionych haseł z wycieków, ataki na hasła metodą prób, nadużywanie powiadomień logowania dwuetapowego (powtarzające się fałszywe powiadomienia); pokaz różnicy między kontem z i bez uwierzytelniania wieloskładnikowego.
4. **Złośliwe oprogramowanie i zagrożenia przeglądarkowe** – Złośliwe rozszerzenia, fałszywe aktualizacje, automatyczne pobieranie złośliwych plików; przykładowa analiza złośliwego załącznika w środowisku testowym Wykonawcy.
5. **Nowe zagrożenia wykorzystujące sztuczną inteligencję** –
 - wykorzystanie fałszywych nagrań głosu/obrazu (deepfake) w oszustwach „na przełożonego” – pokaz przykładów, omówienie sygnałów ostrzegawczych,
 - wiarygodny phishing generowany przez narzędzia AI – bardziej przekonujące treści, język „urzędowy”,
 - wycieki danych z asystentów AI – jak użytkownik może się chronić (nie wklejać treści wrażliwych, stosować się do polityk),
 - fałszywe tożsamości i profile – proste metody weryfikacji (telefon zwrotny, kontakt innym kanałem).
6. **Bezpieczne nawyki użytkownika** – Aktualizacje systemów i aplikacji, zasada minimalnych uprawnień, blokowanie stanowiska pracy, zasady zgłaszania podejrzanych zdarzeń zgodnie z procedurami SZBI.

Forma i metody: wykład z przykładami, demonstracje na żywo w środowisku laboratoryjnym Wykonawcy, krótkie ćwiczenia decyzyjne („co byś zrobił/a w tej sytuacji?”), sesja pytań i odpowiedzi.

Czas trwania:

- wariant rozdzielnny – min. 5 godz. dydaktycznych na grupę,
- wariant 1-dniowy (A+B łącznie) – realizacja efektów uczenia zadania B w ramach co najmniej 7 godzin łącznego czasu dnia.

Wykonawca zapewnia pełne odseparowanie demonstracji od infrastruktury produkcyjnej Zamawiającego (środowisko laboratoryjne, własny sprzęt i łącze), bez wysyłki rzeczywistych wiadomości do użytkowników.

5.3. Zadanie C – Kadra kierownicza: wdrożenie i nadzór nad SZBI

Cel: przygotowanie kierownictwa do sprawowania nadzoru nad systemem bezpieczeństwa informacji oraz do podejmowania decyzji w oparciu o zarządzanie ryzykiem, wymagania KRI i normy ISO.

Zakres:

1. **Rola kierownictwa w SZBI i KRI** – Przywództwo, odpowiedzialność za politykę bezpieczeństwa, cele, zasoby i przegląd SZBI.

2. **Zarządzanie ryzykiem** – Podstawy analizy i oceny ryzyka, akceptacja ryzyk, powiązanie wyników analizy ryzyka z decyzjami inwestycyjnymi i priorytetami działań.
3. **Polityki i procedury SZBI, zgodność i odpowiedzialności** – Przegląd kluczowych dokumentów (polityki, instrukcje, procedury incydentowe i ciągłości działania); rola administratora danych, inspektora ochrony danych, kierownictwa i pracowników; najważniejsze wymagania KRI i przepisów o ochronie danych z perspektywy zarządczej.
4. **Nadzór nad incydentami i doskonaleniem** – Cykl ciągłego doskonalenia w bezpieczeństwie informacji; przegląd zarządzania; raportowanie incydentów i działań naprawczych; wykorzystanie wniosków z incydentów do poprawy SZBI.
5. **Ciągłość działania** – Wprowadzenie do planów ciągłości działania i odtwarzania po awarii; podstawowe parametry (dopuszczalny czas i zakres utraty danych); proste ćwiczenie scenariuszowe (np. atak ransomware w urzędzie, awaria łączności).
6. **Kultura bezpieczeństwa i komunikacja** – Znaczenie postawy kierownictwa wobec bezpieczeństwa; budowanie kultury zgłaszania błędów i incydentów bez „szukania winnych”; przykładowe komunikaty wewnętrzne i działania budujące świadomość.

Forma i metody: warsztat z przykładami z sektora publicznego, studia przypadków, dyskusja moderowana.

Czas trwania: min. 6 godz. dydaktycznych (1 dzień) dla jednej grupy.

5.4. Zadanie D – Informatycy / zespół IT: wdrożenie i utrzymanie SZBI

Cel: przygotowanie zespołu IT do praktycznego wdrażania i utrzymania kontroli bezpieczeństwa zgodnie z wymaganiami KRI, normami ISO 27001/27002 i dobrymi praktykami, w tym do współpracy z kierownictwem i inspektorem ochrony danych.

Zakres (warsztaty techniczno-procesowe):

1. **Zarządzanie tożsamością i dostępem** – Zasada najmniejszych uprawnień; przeglądy dostępów; konta uprzywilejowane; uwierzytelnianie wieloskładnikowe (w tym klucze sprzętowe); przykładowe procedury nadawania i odbierania uprawnień.
2. **Wzmacnianie bezpieczeństwa systemów (hardening)** – Podstawowe zalecenia konfiguracyjne dla systemów Windows/Linux, zarządzanie poprawkami bezpieczeństwa, zarządzanie hasłami kont lokalnych; segmentacja sieci (podział na strefy bezpieczeństwa).
3. **Bezpieczeństwo poczty elektronicznej i domen** – Konfiguracja mechanizmów uwierzytelniania poczty (SPF, DKIM, DMARC) chroniących przed podszywaniem się pod domenę Zamawiającego; wykorzystanie mechanizmów pocztowych w ochronie przed phishingiem.
4. **Monitoring i wykrywanie zagrożeń** – Logowanie i korelacja zdarzeń; przykładowe scenariusze – oszustwo mailowe, ransomware, wyciek danych do chmury; ćwiczenia z analizy logów w środowisku testowym Wykonawcy.
5. **Zarządzanie podatnościami** – Inwentaryzacja aktywów (sprzęt, oprogramowanie, usługi); skanowanie podatności; ocena ryzyka podatności; planowanie i wykonywanie działań naprawczych.
6. **Kopie zapasowe** – Zasada co najmniej trzech kopii na dwóch nośnikach z jedną kopią odporną na ransomware; testy odtworzeniowe; powiązanie wymagań dot. kopii z KRI i SZBI.
7. **Reagowanie na incydenty** – Przygotowanie i stosowanie prostych procedur obsługi incydentów (klasyfikacja, izolacja, komunikacja, dokumentowanie); wzory raportów i materiału dowodowego do analiz i audytów.

8. **Bezpieczeństwo danych** – Stosowanie szyfrowania (dane w spoczynku i w transmisji), klasyfikacja danych i etykiety poufności, zasady retencji i archiwizacji danych w systemach IT.
9. **AI w pracy administratora IT** – Zasady bezpiecznego korzystania z narzędzi AI do generowania skryptów, konfiguracji, dokumentacji; ryzyka nieświadomego ujawnienia konfiguracji lub topologii sieci; dobre praktyki maskowania danych.
10. **Nowo zakupione systemy teleinformatyczne** – Bezpieczna konfiguracja po wdrożeniu; wykorzystanie wbudowanych funkcji bezpieczeństwa (uwierzytelnianie wieloskładnikowe, role i uprawnienia, logowanie, szyfrowanie, alerty); przygotowanie list kontrolnych na etapie odbioru; uwzględnienie wymogów bezpieczeństwa w dokumentacji zamówień.

Forma i metody: warsztat z elementami laboratorium (praca na środowisku testowym Wykonawcy), demonstracje konfiguracji, ćwiczenia praktyczne.

Czas trwania: min. 1 dzień (8 godz. dydaktycznych); Zamawiający dopuszcza oferty 1–2-dniowe (8–16 godz.), z niezmienionym zakresem merytorycznym.

6. Wymogi organizacyjne i jakościowe

6.1. Analiza potrzeb

Przed rozpoczęciem cyklu szkoleń Wykonawca przeprowadzi analizę potrzeb (wywiad z przedstawicielami Zamawiającego, min. 90 minut), w formie stacjonarnej lub zdalnej, w innym dniu niż szkolenie. W ciągu 2 dni roboczych od analizy Wykonawca przedłoży szczegółowy plan szkoleń (harmonogram + doprecyzowany program) do akceptacji Zamawiającego. Z analizy sporządzony zostanie krótki protokół z rekomendacjami. Czas analizy nie wlicza się do godzin szkoleniowych.

6.2. Materiały szkoleniowe

Materiały dla uczestników w formie elektronicznej (PDF), obejmujące slajdy lub skrypt oraz krótkie kompendium najważniejszych zasad (szczególnie dla zadań A i B). Na życzenie Zamawiającego – możliwość dostarczenia wydruków. Materiały przygotowane w sposób umożliwiający powiększanie i wydruk w dobrej jakości. Materiały będą zgodne ze „Standardami dostępności dla polityki spójności 2021-2027”.

Zamawiający nabywa niewyłączną, nieograniczoną terytorialnie i czasowo licencję na wykorzystywanie otrzymanych materiałów szkoleniowych (PDF) na potrzeby wewnętrzne (szkolenia nowych pracowników, utrwalanie wiedzy) bez dodatkowych opłat. Licencja obejmuje prawo do kopiowania, udostępniania wewnętrznego i drukowania materiałów na potrzeby pracowników Zamawiającego i jego jednostek organizacyjnych.

6.3. Ścieżka uzupełniająca (osoby nieobecne i nowo zatrudnieni)

W celu przeszkolenia osób nieobecnych na szkoleniach stacjonarnych oraz nowo zatrudnionych (do 30.06.2026 r.) Wykonawca zapewni:

- komplet materiałów szkoleniowych (PDF) przekazanych Zamawiającemu do samodzielnego udostępniania pracownikom,
- zestaw pytań testowych (min. 10 pytań dla zadania A i min. 10 pytań dla zadania B) w formie umożliwiającej przeprowadzenie testu przez Zamawiającego (np. formularz online lub plik do wydruku).

Opcjonalnie Wykonawca może zaproponować w ofercie rozszerzenie ścieżki uzupełniającej o nagrania wideo lub kurs e-learningowy, z osobną wyceną. Zamawiający oceni zasadność rozszerzenia w kontekście budżetu.

Dla osób uczestniczących stacjonarnie ścieżka uzupełniająca ma charakter nieobowiązkowy (materiał do utrwalenia wiedzy).

6.4. Ewaluacja – testy wiedzy (pre-test i post-test)

Dla zadań A i B Wykonawca przygotowuje dwa odrębne zestawy pytań testowych:

- **pre-test** (przed szkoleniem, na początku dnia szkoleniowego, ok. 10–15 min) – min. 10 pytań badających wyjściowy poziom świadomości pracowników (ogólna wiedza o zagrożeniach, rozpoznawanie ryzykownych sytuacji, podstawowe nawyki bezpieczeństwa),
- **post-test** (po szkoleniu, na zakończenie dnia szkoleniowego, ok. 10–15 min) – min. 10 pytań osadzonych w treściach omawianych podczas szkolenia (procedury, scenariusze, zasady SZBI); pytania o innej treści niż pre-test, ale badające ten sam obszar kompetencji na wyższym poziomie szczegółowości.

Oba zestawy powinny mieć zbliżony poziom trudności, lecz różnić się treścią pytań, tak aby post-test mierzył przyswojenie wiedzy przekazanej na szkoleniu, a nie zapamiętanie odpowiedzi z pre-testu.

Testy mają charakter diagnostyczny – ich wyniki nie warunkują odbioru szkolenia, lecz służą ocenie efektywności szkolenia. Wyniki obu testów (zbiorczy odsetek poprawnych odpowiedzi przed i po szkoleniu, z podziałem na zadania A i B) zostaną porównane w raporcie z ewaluacji.

Dla zadań C i D – ankieta ewaluacyjna (min. 10 pytań).

Dodatkowo dla wszystkich zadań – ankieta ewaluacyjna oceniająca jakość szkolenia (min. 10 pytań).

W ciągu 14 dni od zakończenia cyklu Wykonawca przekaze Zamawiającemu zbiorczy raport z ewaluacji zawierający:

- porównanie wyników pre-testów i post-testów (zadania A i B),
- porównanie wyników symulacji phishingowych nr 1 i nr 2 (pkt 6.9),
- podsumowanie ankiet ewaluacyjnych,
- wnioski i rekomendacje,
- dane przydatne do rozliczenia wskaźników projektu grantowego, w szczególności liczbę przeszkolonych pracowników z podziałem na jednostki organizacyjne, typ szkolenia i płeć uczestników.

6.5. Zaświadczenia

Imienne zaświadczenia dla wszystkich uczestników, z podaniem nazwy szkolenia, zakresu tematycznego i liczby godzin.

6.6. Dostępność

Zapewnienie dostępności szkoleń dla osób ze szczególnymi potrzebami (m.in. możliwość powiększania materiałów, odpowiednio przygotowana sala, możliwość udziału z asystą).

6.7. Oznaczenia projektu

Wszystkie materiały, zaświadczenia i listy obecności oznaczone zgodnie z wytycznymi FERC/UE, z informacją o współfinansowaniu.

6.8. Bezpieczeństwo demonstracji

Pokazy ataków (zadania B i D) realizowane wyłącznie w środowisku odizolowanym (laboratorium Wykonawcy), bez łączenia z siecią produkcyjną Zamawiającego.

6.9. Kontrolowana symulacja phishingowa (pomiar świadomości)

Wykonawca we współpracy z Zamawiającym przeprowadzi dwie kontrolowane symulacje phishingowe skierowane do pracowników objętych szkoleniami:

- **symulacja nr 1** – przed rozpoczęciem cyklu szkoleń stacjonarnych,
- **symulacja nr 2** – po zakończeniu cyklu szkoleń stacjonarnych (do 7 dni po zakończeniu cyklu szkoleń stacjonarnych).

Zakres współpracy:

- Wykonawca przygotowuje scenariusz każdej symulacji (treść wiadomości e-mail, stronę docelową/landing page) i uzgodni go z Zamawiającym przed wysyłką.
- Wykonawca zapewni wsparcie techniczne przy konfiguracji narzędzia do symulacji phishingowej (instalacja, konfiguracja kampanii, uruchomienie).
- **Wysyłka wiadomości testowych odbywa się z infrastruktury Zamawiającego** – Wykonawca nie otrzymuje listy adresów e-mail pracowników. Zamawiający (zespół IT) wprowadza adresy e-mail do narzędzia i uruchamia wysyłkę.

Warunki symulacji:

- wiadomości nie zawierają złośliwego oprogramowania ani nie wykonują żadnych operacji na urządzeniach odbiorców — służą wyłącznie rejestracji faktu kliknięcia w link lub otwarcia załącznika testowego,
- wyniki symulacji (odsetek pracowników, którzy kliknęli w link — bez danych identyfikujących konkretne osoby) zostaną przedstawione w raporcie z ewaluacji jako wskaźnik zmiany poziomu świadomości,
- szczegóły techniczne realizacji (wybór narzędzia, sposób instalacji, konfiguracja) zostaną uzgodnione między Wykonawcą a Zamawiającym w ramach analizy potrzeb (pkt 6.1) lub w ciągu 14 dni od zawarcia umowy.

6.10. Miejsce realizacji szkoleń

Szkolenia stacjonarne odbywają się w siedzibie Zamawiającego. Zamawiający udostępnia salę szkoleniową wyposażoną w rzutnik multimedialny, ekran/telewizor oraz dostęp do zasilania. Wykonawca zapewnia własny sprzęt niezbędny do prowadzenia szkolenia i demonstracji (laptop trenerski, środowisko laboratoryjne, łącze internetowe do demonstracji – niezależne od sieci Zamawiającego).

6.11. Godziny realizacji i harmonogram

Szkolenia realizowane w godzinach pracy Zamawiającego (chyba że strony uzgodnią inaczej); harmonogram uzgodniony co najmniej 7 dni przed terminem pierwszego szkolenia.

6.12. Udział pracowników

Grupy i harmonogram powinny zostać zaplanowane tak, aby zapewnić możliwość udziału wszystkich pracowników przewidzianych do przeszkolenia. Celem jest objęcie szkoleniem 100% pracowników (w trybie stacjonarnym lub poprzez ścieżkę uzupełniającą). Minimalny próg odbioru zamówienia wynosi 95% pracowników przeszkolonych w dowolnej formie — próg uwzględnia absencje losowe (długotrwała choroba, urlop macierzyński/rodzicielski, rozwiązanie stosunku pracy).

7. Harmonogram realizacji

Faza	Termin	Produkt / rezultat
1. Analiza potrzeb + uzgodnienie symulacji phishingowej	do 7 dni roboczych od zawarcia umowy	Protokół z analizy + szczegółowy plan szkoleń + scenariusz symulacji nr 1
2. Symulacja phishingowa nr 1	do 10 dni od zawarcia umowy oraz przed pierwszym szkoleniem stacjonarnym	Wysyłka wiadomości testowych, zebranie wyników
3. Akceptacja planu szkoleń	do 14 dni roboczych od zawarcia umowy	Pisemne zatwierdzenie planu przez Zamawiającego
4. Realizacja szkoleń stacjonarnych	do 30 dni kalendarzowych od zawarcia umowy	Listy obecności, materiały PDF, zaświadczenia, wyniki pre-testów i post-testów
5. Symulacja phishingowa nr 2	do 7 dni po ostatnim szkoleniu stacjonarnym	Wysyłka wiadomości testowych, zebranie wyników
6. Przekazanie materiałów ścieżki uzupełniającej	do 7 dni od zakończenia ostatniego szkolenia stacjonarnego	Materiały PDF + testy dla osób nieobecnych
7. Raport z ewaluacji	do 14 dni od zakończenia ostatniego szkolenia stacjonarnego	Raport zbiorczy z wynikami testów, ankiet, symulacji phishingowych i rekomendacjami

Ścieżka uzupełniająca (materiały PDF + testy) jest dostępna dla nowo zatrudnionych pracowników do dnia 30.06.2026 r.

Dokładne daty i podział na grupy zostaną uzgodnione z Zamawiającym po podpisaniu umowy, z uwzględnieniem organizacji pracy urzędu i jednostek organizacyjnych.

8. Rezultaty

1. Przeszkolenie 74 pracowników (zadania A i B) oraz 9 osób kadry kierowniczej (zadanie C); realizacja szkolenia IT (zadanie D) dla 2 osób.
2. Zestaw materiałów szkoleniowych (PDF) wraz z kompendium najważniejszych zasad.
3. Przeprowadzenie dwóch kontrolowanych symulacji phishingowych (przed i po cyklu szkoleń).
4. Raport z ewaluacji (porównanie wyników pre-testów i post-testów, porównanie wyników symulacji phishingowych, podsumowanie ankiet) wraz z rekomendacjami.
5. Listy obecności oraz rejestr wydanych zaświadczeń.
6. Materiały ścieżki uzupełniającej (PDF + testy) do wykorzystania przez Zamawiającego.

9. Wymagania wobec Wykonawcy (warunki udziału / personel)

9.1. Doświadczenie

Wykonawca musi posiadać co najmniej 2-letnie doświadczenie w przygotowaniu i przeprowadzeniu szkoleń z obszaru bezpieczeństwa informacji lub cyberbezpieczeństwa. W ostatnich 2 latach przed terminem składania ofert Wykonawca zrealizował co najmniej 2 usługi szkoleniowe z tego obszaru dla podmiotów publicznych, w tym:

- min. 1 usługę obejmującą kadrę kierowniczą,
- min. 1 usługę obejmującą zespoły IT / administratorów.

9.2. Personel szkoleniowy

Co najmniej 2 trenerów, w tym:

- jeden z certyfikatem typu ISO/IEC 27001 Lead Auditor lub Lead Implementer (lub równoważnym) oraz doświadczeniem min. 2 lata w prowadzeniu szkoleń z zakresu bezpieczeństwa informacji lub SZBI,
- jeden z doświadczeniem technicznym min. 2 lata w obszarze bezpieczeństwa IT (np. administracja bezpieczeństwa, obsługa incydentów, zarządzanie podatnościami, administracja systemami).

Każdy z trenerów musi posiadać min. 30 godzin doświadczenia szkoleniowego z zakresu bezpieczeństwa informacji, cyberbezpieczeństwa lub SZBI w ciągu ostatnich 2 lat przed terminem składania ofert.

9.3. Sprzęt i środowisko laboratoryjne

Zapewnienie sprzętu i oprogramowania niezbędnego do pokazów i ćwiczeń (środowisko laboratoryjne), w tym maszyn wirtualnych; środowisko odseparowane od infrastruktury Zamawiającego.

9.4. Informacje wymagane z ofertą

Wraz z ofertą Wykonawca przedstawi:

- **zarys programu (sylabus) dla zadań A–D,**
- **krótkie CV trenerów (z opisem doświadczenia, w tym w sektorze publicznym).**

9.5. Poufność

Oświadczenia o zachowaniu poufności trenerów i innych osób zaangażowanych w realizację; zakaz używania realnych danych Zamawiającego w środowisku demonstracyjnym.

9.6. Osoby kluczowe i podwykonawcy

Wykonawca wskaże imiennie osoby kluczowe (trenerów), a ewentualnych podwykonawców – z równoważnymi kwalifikacjami. Zamawiający zastrzega prawo do żądania poświadczeń kwalifikacji i referencji.

Zmiana trenera wskazanego w ofercie wymaga uprzedniej pisemnej zgody Zamawiającego. Wykonawca może proponować zmianę wyłącznie na osobę posiadającą kwalifikacje i doświadczenie co najmniej równoważne z kwalifikacjami i doświadczeniem trenera zastępowanego (w tym nie niższe niż wymagane minimum określone w pkt 9.2).

10. Kryteria odbioru

1. Dostarczenie programów szkoleń (dla zadań A–D) i harmonogramu zaakceptowanych przez Zamawiającego.
2. Zrealizowanie minimalnych czasów trwania i zakresów tematycznych określonych w rozdziale 5.
3. Przeszkolenie min. 95% pracowników przewidzianych do udziału (w trybie stacjonarnym lub poprzez ścieżkę uzupełniającą). Zamawiający zapewni dostępność szkolenia dla 100% pracowników; próg 95% stanowi minimalny warunek odbioru uwzględniający absencje losowe.
4. Przeprowadzenie pre-testów i post-testów (zadania A i B) oraz ankiet ewaluacyjnych.
5. Przeprowadzenie demonstracji ataków (zadanie B oraz warsztaty w zadaniu D) w sposób bezpieczny i zrozumiały dla uczestników, wyłącznie w środowisku odizolowanym od infrastruktury Zamawiającego.
6. Przeprowadzenie dwóch kontrolowanych symulacji phishingowych (przed i po cyklu szkoleń) we współpracy z Zamawiającym, zgodnie z pkt 6.9.
7. Przekazanie kompletu materiałów szkoleniowych, list obecności, zaświadczeń oraz materiałów ścieżki uzupełniającej (PDF + testy) zgodnie z pkt 6.3.
8. Przekazanie raportu z ewaluacji (w ciągu 14 dni od zakończenia szkoleń stacjonarnych).

11. Zasady rozliczeń

1. Cena ofertowa powinna obejmować całość kosztów związanych z realizacją zamówienia, w szczególności: przygotowanie i realizację szkoleń stacjonarnych, przygotowanie materiałów szkoleniowych, przygotowanie materiałów ścieżki uzupełniającej, zapewnienie środowiska laboratoryjnego i sprzętu demonstracyjnego, przygotowanie scenariuszy i wsparcie techniczne

symulacji phishingowych, przygotowanie pre-testów i post-testów, ewaluację, zaświadczenia dla uczestników.

2. Wykonawca wyodrębni na fakturze (lub w załączniku stanowiącym integralną część faktury) pozycje umożliwiające przypisanie kosztów do poszczególnych jednostek organizacyjnych i typów szkoleń, zgodnie z tabelą zakresu rzeczowego zamówienia (rozdział 2) i podziałem cenowym z formularza ofertowego. W szczególności faktura musi umożliwiać rozdzielenie kosztów na:
 - o UMiG, MGZO, ZUWiK, MGOPS,
 - o typ szkolenia: bezpieczeństwo informacji (zadanie A), cyberbezpieczeństwo z pokazami (zadanie B), kadra kierownicza (zadanie C), zespół IT (zadanie D).
3. Zamawiający informuje, że zamówienie jest finansowane w ponad 70% ze środków publicznych. Usługi szkoleniowe mogą podlegać zwolnieniu z VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy o podatku od towarów i usług. Wykonawca zobowiązany jest do prawidłowego określenia stawki VAT w ofercie.
4. Odbiór merytoryczny opiera się na spełnieniu kryteriów odbioru określonych w rozdziale 10.

12. Kryterium oceny ofert

Zamawiający dokona oceny ofert na podstawie jednego kryterium:

Kryterium	Waga	Maks. punktów
Cena brutto (C)	100%	100

Punkty obliczane wg wzoru:

$$C = (\text{najniższa cena brutto} / \text{cena badanej oferty}) \times 100$$

Pod uwagę brana jest łączna cena brutto oferty (suma pozycji 1–13 z formularza ofertowego). Oferta najtańsza otrzymuje 100 pkt.

Zamówienie zostanie udzielone Wykonawcy, którego oferta uzyska najwyższą liczbę punktów (tj. zaoferuje najniższą cenę brutto) spośród ofert niepodlegających odrzuceniu.

Uzasadnienie zastosowania kryterium 100% ceny: Przedmiot zamówienia ma ustalone standardy jakościowe – wymagania merytoryczne, minimalne czasy trwania, zakresy tematyczne, wymagania wobec personelu szkoleniowego (kwalifikacje i doświadczenie) oraz kryteria odbioru zostały szczegółowo określone w niniejszym OPZ (rozdziały 5, 9 i 10). Jakość realizacji jest zapewniona poprzez warunki udziału w postępowaniu.

13. CPV (Słownik zamówień)

- 80500000-9 – Usługi szkoleniowe
- 80510000-2 – Różne usługi szkoleniowe
- 80530000-8 – Usługi szkolenia zawodowego
- 80570000-0 – Usługi szkolenia w dziedzinie bezpieczeństwa

14. Postanowienia dot. ochrony danych i informacji

1. Wykonawca zapewni zgodność przetwarzania danych osobowych (m.in. listy obecności, testy, ankiety) z przepisami o ochronie danych osobowych; w razie potrzeby zawarta zostanie umowa powierzenia przetwarzania danych.
2. Zabrania się wykorzystywania realnych danych Zamawiającego (np. danych osobowych, rzeczywistych dokumentów, konfiguracji systemów produkcyjnych) w środowisku demonstracyjnym; środowisko laboratoryjne musi być odizolowane od infrastruktury Zamawiającego.
3. W ramach symulacji phishingowych (pkt 6.9) adresy e-mail pracowników nie są przekazywane Wykonawcy – wprowadzanie adresów do narzędzia i wysyłka wiadomości testowych leży po stronie Zamawiającego.

15. Dostępność i równość szans

1. Wykonawca zapewni dostępność szkoleń i materiałów dla osób ze szczególnymi potrzebami, w szczególności osób z niepełnosprawnościami (m.in. możliwość powiększania treści, odpowiedni kontrast, czytelne czcionki, zapewnienie odpowiednich warunków w sali).
2. Realizacja zamówienia odbywa się z poszanowaniem zasady równości szans kobiet i mężczyzn oraz niedyskryminacji ze względu na jakąkolwiek przesłankę.
3. Realizacja zamówienia będzie odbywać się zgodnie ze „Standardami dostępności dla polityki spójności 2021-2027”.

16. Informacje końcowe

1. W sprawach nieuregulowanych niniejszym OPZ zastosowanie mają właściwe przepisy ustawy Prawo zamówień publicznych oraz wytyczne konkursu „Cyberbezpieczny Samorząd”.
2. Złożenie oferty jest równoznaczne z akceptacją treści niniejszego OPZ.

II Termin realizacji zamówienia:

2 m-ce od dnia podpisania umowy.

III Warunki płatności:

Przelew 14 dni, od daty dostarczenia Zamawiającemu poprawnie wystawionej faktury wraz z podpisanym przez obie Strony protokołem odbioru.

IV Kryterium wyboru ofert:

najniższa cena brutto – znaczenie 100%

1. Wybrana zostanie najkorzystniejsza oferta zawierająca najniższą cenę (jako cenę należy rozumieć kwotę brutto za wykonanie w całości zamówienie),
2. 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.

3. 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,

V Miejsce i termin składania ofert:

Ofertę należy złożyć w Urzędzie Miasta i Gminy Kaczory, ul. Piłska 1, pok. nr 18, do dnia 23 lutego 2026 r. do godziny 15.00 . Istnieje możliwość przesłania oferty drogą mailową na adres: inwestycje@kaczory.pl.

Otwarcie ofert nastąpi w dniu 23 lutego 2026 r. o godz. 15.15.

VI Uwagi końcowe:

- niniejsze zapytanie ofertowe nie stanowi zobowiązania Miasta i Gminy Kaczory do zawarcia umowy,
- Miasto i Gmina Kaczory zastrzega sobie prawo do unieważnienia postępowania bez podania przyczyny;

VII 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

Signature Not Verified

Dokument podpisany przez Brunon
Wolski; Miasto i Gmina Kaczory
Data: 2026.02.16 15:21:35 CET

