OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

Załącznik nr 1 do Zapytania Ofertowego nr 7/CW/0082

Audyt końcowy zgodności z wymaganiami Krajowych Ram Interoperacyjności (KRI) oraz ustawy o krajowym systemie cyberbezpieczeństwa (uoKSC).

Nr projektu grantowego	KPOD.05.10-CW.01-001/25/0082
Program	KPO, Inwestycja C3.1.1 Cyberbezpieczeństwo – CyberPL, nabór KPOD.05.10-CW.01-001/25
Konkurs	Cyberbezpieczne Wodociągi
Nr postępowania	7/CW/0082
Data opracowania	listopad 2026 r.
Wersja	1.0

I. Informacje ogólne

1.1. Zamawiający

Nazwa	**Zakład Wodociągów i Kanalizacji Police Sp. z o.o.**
Adres	ul. Grzybowa 50, 72-010 Police
NIP	8513212846
REGON	368109625
KRS	0000692181
Telefon / e-mail	+48 91 424 13 10 / sekretariat@zwikpolice.pl
Osoba do kontaktu w postępowaniu	Michał Janas, e-mail: biuro@mjc.com.pl

1.2. Kontekst projektu

Niniejszy Opis Przedmiotu Zamówienia (OPZ) stanowi podstawę przeprowadzenia postępowania o udzielenie zamówienia przez Zakład Wodociągów i Kanalizacji Police Sp. z o.o. (dalej: Zamawiający) w ramach realizacji projektu grantowego pn. „Wzmocnienie cyberbezpieczeństwa infrastruktury w Zakładzie Wodociągów i Kanalizacji Police Sp. z o.o.”, dofinansowanego z Krajowego Planu Odbudowy i Zwiększania Odporności (KPO), Inwestycja C3.1.1 Cyberbezpieczeństwo – CyberPL, nabór nr KPOD.05.10-CW.01-001/25, na podstawie Umowy o powierzenie grantu nr KPOD.05.10-CW.01-001/25/0082/KPOD.05.10-CW.01-001/25/2026.

Zamawiający jest przedsiębiorstwem komunalnym, którego jedynym udziałowcem jest Gmina Police. Zamawiający zarządza i eksploatuje kluczową infrastrukturę wodociągowo-kanalizacyjną, w tym Stację Uzdatniania Wody oraz przepompownie

ścieków, i jako przedsiębiorstwo wodociągowo-kanalizacyjne jest podmiotem krajowego systemu cyberbezpieczeństwa (operatorem usługi kluczowej / podmiotem kluczowym sektora wody pitnej) w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. 2026 poz. 20 ze zm., w brzmieniu nadanym ustawą z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, Dz.U. 2026 poz. 252 – dalej: „ustawa o KSC"). Zamawiający jest zobowiązany do wdrożenia środków zarządzania ryzykiem cyberbezpieczeństwa zgodnie z dyrektywą NIS2 (2022/2555/UE) oraz wymaganiami Regulaminu Konkursu Grantowego.

Zamawiający eksploatuje infrastrukturę obejmującą zarówno systemy informatyczne (IT), jak i systemy technologii operacyjnej (OT/ICS/SCADA) służące uzdatnianiu i dystrybucji wody oraz odbiorowi ścieków. Zakres przedmiotu zamówienia uwzględnia specyfikę obu tych środowisk.

1.3. Brak podziału zamówienia na części

Zamówienie nie zostało podzielone na części. Przedmiotem zamówienia jest jedna usługa audytu końcowego zgodności z wymaganiami KRI i ustawy o KSC (kategoria kosztów KPO U25), przeprowadzanego przez wykonawcę niezależnego od podmiotu, który na zlecenie Zamawiającego opracował i wdrożył System Zarządzania Bezpieczeństwem Informacji (SZBI) Zamawiającego, oraz od podmiotu, któremu Zamawiający powierzył lub powierzy przegląd i aktualizację SZBI w ramach Projektu grantowego (dalej łącznie: „Wykonawca SZBI").

1.4. Wymagania ogólne

1) Wszystkie dokumenty, raporty i prezentacje wytworzone w ramach zamówienia muszą być oznakowane zestawieniem znaków graficznych obejmującym: Godło Rzeczypospolitej Polskiej, flagę Unii Europejskiej z napisem „Sfinansowane przez Unię Europejską – NextGenerationEU", logo Krajowego Planu Odbudowy i Zwiększania Odporności oraz logo Centrum Projektów Polska Cyfrowa (CPPC) – zgodnie z aktualnymi Wytycznymi dotyczącymi informacji i promocji dla KPO. Wzory stron tytułowych z układem logotypów wymagają uprzedniej akceptacji Koordynatora Projektu.
2) Wszystkie materiały i dokumenty przekazywane w formie elektronicznej muszą spełniać wymagania dostępności cyfrowej na poziomie WCAG 2.1 AA (lub standardu równoważnego), określone w Załączniku nr 2 „Standardy dostępności dla polityki spójności 2021–2027" do Wytycznych dotyczących realizacji zasad równościowych w ramach funduszy unijnych na lata 2021–2027, w szczególności: aktywną warstwę tekstową w plikach PDF (zakaz dostarczania płaskich skanów), otagowanie plików PDF, uporządkowaną strukturę nagłówków, opisy alternatywne grafik oraz kontrast nie niższy niż 4,5:1. Wymóg ten nie

dotyczy zrzutów ekranu stanowiących dowód techniczny oraz aneksów zawierających surowe wyniki narzędzi, dla których Wykonawca zapewnia opis tekstowy w części głównej raportu.

3) Wszystkie dokumenty i produkty przekazywane są w wersji elektronicznej, w formatach edytowalnych (.docx, .xlsx lub równoważnych, np. .odt, .ods) oraz – tam gdzie wymagane – w formacie PDF lub równoważnym.
4) Wszystkie produkty muszą być sporządzone w języku polskim, w formalnym stylu właściwym dla dokumentacji systemu zarządzania, i muszą być w pełni dostosowane do specyfiki Zamawiającego jako przedsiębiorstwa wodociągowo-kanalizacyjnego. Niedopuszczalne jest dostarczanie szablonów lub dokumentów generycznych bez adaptacji do realiów organizacji Zamawiającego.
5) Realizacja przedmiotu zamówienia musi być zgodna z zasadą „nie czyń znaczącej szkody” (DNSH) w rozumieniu art. 17 rozporządzenia (UE) 2020/852 oraz z wytycznymi obowiązującymi w ramach KPO.
6) Wykonawca i wszystkie osoby zaangażowane w realizację zamówienia zobowiązani są do zachowania w ścisłej tajemnicy wszelkich informacji uzyskanych w toku realizacji zamówienia, w szczególności danych o infrastrukturze IT i OT/SCADA, danych osobowych pracowników i klientów, wyników analizy ryzyka oraz wszystkich dokumentów wewnętrznych Zamawiającego. Obowiązek poufności obowiązuje przez cały okres realizacji zamówienia oraz przez okres 5 lat po jego zakończeniu, a w odniesieniu do informacji stanowiących tajemnicę przedsiębiorstwa Zamawiającego – bezterminowo. Wykonawca zobowiązany jest do zawarcia umów o zachowaniu poufności (NDA) ze wszystkimi osobami zaangażowanymi w realizację zamówienia.
7) Wszelkie autorskie prawa majątkowe do dokumentacji, raportów i innych utworów wytworzonych w ramach realizacji zamówienia przechodzą na Zamawiającego z chwilą podpisania protokołu odbioru danego produktu, na zasadach szczegółowo określonych we wzorze umowy.
8) Wykonawca zobowiązany jest poddać się kontrolom i audytom prowadzonym przez Zamawiającego, CPPC, NASK – Państwowy Instytut Badawczy, ministra właściwego do spraw informatyzacji, Instytucję Koordynującą KPO, Szefa Krajowej Administracji Skarbowej, Najwyższą Izbę Kontroli, Komisję Europejską, Europejski Trybunał Obrachunkowy oraz OLAF, a także przechowywać dokumentację realizacji zamówienia nie krócej niż do dnia 31 grudnia 2031 r.

1.5. Podstawy prawne i normatywne

- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tj. Dz.U. 2026 poz. 20 ze zm.);

- Ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz.U. 2026 poz. 252);
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. (NIS2);
- Norma ISO/IEC 27001:2022 (lub norma równoważna), której polskim wdrożeniem jest norma PN-EN ISO/IEC 27001:2023 (lub norma równoważna);
- Norma ISO/IEC 27002:2022 (lub norma równoważna) – praktyki zarządzania bezpieczeństwem informacji;
- Norma ISO/IEC 27005:2022 (lub norma równoważna) – zarządzanie ryzykiem bezpieczeństwa informacji;
- Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności (Dz.U. 2024 poz. 773);
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO) oraz ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;
- Ustawa z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków;
- Regulamin Konkursu Grantowego „Cyberbezpieczne Wodociągi" (nabór KPOD.05.10-CW.01-001/25) wraz z załącznikami;
- Zasady kwalifikowania wydatków w Przedsięwzięciach realizowanych w ramach Inwestycji C3.1.1 KPO wraz z Załącznikiem nr 1;
- Wytyczne dotyczące informacji i promocji dla Krajowego Planu Odbudowy i Zwiększania Odporności;
- Wytyczne dotyczące realizacji zasad równościowych w ramach funduszy unijnych na lata 2021–2027, w tym Załącznik nr 2 „Standardy dostępności dla polityki spójności 2021–2027".

1.6. Słownik pojęć

Pojęcie	Definicja
SZBI	System Zarządzania Bezpieczeństwem Informacji – zorganizowane podejście do ustanawiania, wdrażania, utrzymywania i ciągłego doskonalenia bezpieczeństwa informacji, zgodne z normą ISO/IEC 27001:2022 (lub normą równoważną).
Koordynator Projektu (KP)	Wyznaczony przez Zamawiającego pracownik posiadający uprawnienia decyzyjne w zakresie bieżącej koordynacji realizacji zamówienia; jedyny adresat komunikacji Wykonawcy.
Produkt	Dokument, raport lub inny rezultat prac Wykonawcy podlegający formalnemu odbiorowi przez Zamawiającego.
Audytor	Każda z osób przeprowadzających audyt zgodności KRI/uoKSC w imieniu Wykonawcy, spełniająca wymagania art. 15 ust. 2 i 2a ustawy o KSC oraz pkt 6.4 i 13.3 Zapytania Ofertowego.
Wykonawca SZBI	Podmiot, który na zlecenie Zamawiającego opracował i wdrożył System Zarządzania Bezpieczeństwem Informacji (SZBI)

Pojęcie	Definicja
	Zamawiającego, oraz podmiot, któremu Zamawiający powierzył lub powierzy przegląd i aktualizację SZBI w ramach Projektu grantowego.
SoA	Deklaracja Stosowania (Statement of Applicability) – dokument wymieniający wszystkie zabezpieczenia Załącznika A normy ISO/IEC 27001:2022 (lub normy równoważnej) wraz z uzasadnieniem ich stosowania lub wyłączenia.
RTP	Plan Postępowania z Ryzykiem (Risk Treatment Plan).
KRI	Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności (Dz.U. 2024 poz. 773).
Środowisko OT/ICS/SCADA	System sterowania i nadzoru nad procesami technologicznymi uzdatniania i dystrybucji wody oraz odbioru ścieków, w tym sterowniki PLC/RTU, stacje operatorskie SCADA oraz sieci przemysłowe.
CSIRT	Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego właściwy dla Zamawiającego zgodnie z ustawą o KSC.
System S46	System teleinformatyczny służący do zgłaszania incydentów do właściwego CSIRT, o którym mowa w ustawie o KSC.
CPPC	Centrum Projektów Polska Cyfrowa z siedzibą w Warszawie – Operator Obsługujący Wnioski w rozumieniu Regulaminu Konkursu Grantowego.
KSeF	Krajowy System e-Faktur, o którym mowa w ustawie z dnia 11 marca 2004 r. o podatku od towarów i usług.
RODO	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.
Dni robocze	Dni od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy w Rzeczypospolitej Polskiej.

1.7. Terminy realizacji

Termin realizacji zamówienia wynika z terminu zakończenia realizacji zakresu rzeczowego Projektu grantowego oraz z końca okresu kwalifikowalności wydatków przypadającego na dzień 31 grudnia 2026 r.

Zakres	Termin
Pozycja 1.1 – audyt zgodności KRI/uoKSC wraz z Raportem z Audytu Zgodności	do 28.12.2026 r.**;** **Protokół Odbioru Końcowego – do 29.12.2026 r.**

II. Audyt końcowy zgodności z KRI i ustawą o KSC

Pozycja 1.1 – Audyt zgodności z KRI i ustawą o KSC (U25)

Kategoria KPO	U25 – Audyt SZBI, audyt SZCD, audyt zgodności KRI/uoKSC przez wykwalifikowanych audytorów
Zakres	Audyt zgodności systemu zarządzania bezpieczeństwem informacji

	Zamawiającego z wymaganiami KRI oraz ustawy o KSC
Wykonawca czynności	co najmniej dwóch audytorów spełniających wymagania art. 15 ust. 2 i 2a ustawy o KSC oraz pkt 6.4 Zapytania Ofertowego (albo akredytowana jednostka oceniająca zgodność), niezależnych od Wykonawcy SZBI i od zespołu opracowującego i aktualizującego dokumentację SZBI
Termin	po zgłoszeniu przez Zamawiającego gotowości do audytu, po zakończeniu przeglądu i aktualizacji SZBI przez Wykonawcę SZBI, nie później niż do 28 grudnia 2026 r.

1. Przedmiot i cel zamówienia

Przedmiotem zamówienia jest przeprowadzenie audytu zgodności systemu zarządzania bezpieczeństwem informacji Zamawiającego z wymaganiami rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności oraz z obowiązkami wynikającymi z ustawy o KSC i dyrektywy NIS2. Celem audytu jest niezależne potwierdzenie, że wdrożone rozwiązania organizacyjne i techniczne odpowiadają wymaganiom prawa, oraz wskazanie obszarów wymagających działań naprawczych.

Audyt stanowi odrębny, samodzielny produkt zamówienia i nie zastępuje audytu SZBI i zgodności z dyrektywą NIS 2 przeprowadzonego wcześniej w ramach Projektu grantowego. Zakres obu audytów jest rozłączny w następujący sposób: audyt SZBI i NIS 2 weryfikował zgodność wdrożonego SZBI z wymaganiami dyrektywy NIS 2 na etapie jego wdrożenia, natomiast audyt Pozycji 1.1, przeprowadzany po wdrożeniu zabezpieczeń technicznych Projektu grantowego oraz po przeglądzie i aktualizacji SZBI, weryfikuje w odniesieniu do całej organizacji Zamawiającego zgodność z wymaganiami powszechnie obowiązującego prawa (KRI, ustawa o KSC, dyrektywa NIS2). Wykonawca zobowiązany jest zapewnić, aby zakres audytu nie pokrywał się z zakresem audytu SZBI i NIS 2 w sposób prowadzący do podwójnego finansowania tej samej usługi, i wykazać to w Planie Audytu przedkładanym do akceptacji Zamawiającego.

2. Zakres audytu

Audyt obejmuje co najmniej:

1) weryfikację zgodności z wymaganiami § 19 i § 20 rozporządzenia KRI, w szczególności w zakresie: opracowania i aktualizacji regulacji wewnętrznych bezpieczeństwa informacji, inwentaryzacji sprzętu i oprogramowania, przeprowadzania okresowych analiz ryzyka, zarządzania uprawnieniami, szkoleń pracowników, zabezpieczeń przed nieuprawnionym dostępem, zabezpieczeń przed złośliwym oprogramowaniem, zapewnienia kopii zapasowych, monitorowania dostępu do informacji, ochrony przed błędami i utratą informacji oraz zapewnienia rozliczalności działań;

2) weryfikację wypełniania obowiązków wynikających z ustawy o KSC, w szczególności: wdrożenia systemu zarządzania bezpieczeństwem w systemie informacyjnym, zarządzania incydentami i ich zgłaszania do właściwego CSIRT (terminy: wczesne ostrzeżenie ≤ 24 h, zgłoszenie ≤ 72 h, sprawozdanie końcowe ≤ 30 dni), korzystania z Systemu S46, wyznaczenia osoby odpowiedzialnej za kontakt w sprawach cyberbezpieczeństwa, zarządzania ryzykiem łańcucha dostaw oraz stosowania środków zarządzania ryzykiem, o których mowa w art. 21 dyrektywy NIS2;
3) weryfikację zgodności zabezpieczeń środowiska OT/ICS/SCADA z wymaganiami wskazanymi w pkt 1 i 2;
4) weryfikację statusu objęcia zasobów teleinformatycznych Zamawiającego monitoringiem serwisu moje.cert.pl, zgodnie z Umową o powierzenie grantu;
5) przegląd dowodów (zapisów, rejestrów, logów, dokumentów) potwierdzających faktyczne stosowanie zadeklarowanych zabezpieczeń;
6) wywiady z osobami odpowiedzialnymi za poszczególne obszary oraz oględziny wybranych elementów infrastruktury.

3. Sposób realizacji

1) Wykonawca przedkłada Zamawiającemu do akceptacji Plan Audytu, zawierający zakres, kryteria, metodykę, harmonogram czynności audytowych oraz wskazanie audytorów, co najmniej 5 dni roboczych przed rozpoczęciem czynności audytowych.
2) Czynności audytowe realizowane są w siedzibie Zamawiającego, w wymiarze co najmniej 3 dni roboczych obecności audytorów.
3) Audyt kończy się spotkaniem zamykającym z Kierownictwem Zamawiającego, na którym prezentowane są ustalenia audytowe.
4) Audytor zachowuje niezależność i bezstronność; nie może audytować dokumentacji ani rozwiązań, w których opracowaniu lub wdrożeniu uczestniczył, w tym dokumentacji i rozwiązań wytworzonych lub aktualizowanych przez Wykonawcę SZBI. Wykonawca i Audytor składają Oświadczenie o bezstronności i niezależności audytora (Załącznik nr 7 do Zapytania Ofertowego) przed zawarciem umowy oraz ponownie przed rozpoczęciem czynności audytowych; oświadczenie dołącza się także do Raportu z Audytu Zgodności.
5) Czynności audytowe rozpoczynają się po zgłoszeniu przez Zamawiającego gotowości do audytu. Jeżeli z przyczyn niezależnych od Wykonawcy Zamawiający nie zgłosi gotowości w terminie umożliwiającym przeprowadzenie audytu do dnia 28 grudnia 2026 r., audyt przeprowadzany jest w stanie SZBI istniejącym na dzień jego rozpoczęcia, a Raport z Audytu Zgodności wskazuje zakres dokumentacji objętej i nieobjętej wdrożeniem.

4. Produkt Pozycji 1.1

PRODUKT: Raport z Audytu Zgodności KRI/uoKSC

Raport zawiera co najmniej:

(a) zakres, cele, kryteria i metodykę audytu oraz dane audytorów wraz ze wskazaniem posiadanych kwalifikacji i certyfikatów oraz oświadczeniem o bezstronności i niezależności;
(b) wykaz osób, z którymi przeprowadzono wywiady, oraz wykaz przeanalizowanych dokumentów i dowodów;
(c) tabelaryczną ocenę zgodności z każdym wymaganiem KRI i ustawy o KSC objętym zakresem audytu (ZGODNY / NIEZGODNY / CZĘŚCIOWO ZGODNY) wraz z uzasadnieniem i wskazaniem dowodu;
(d) zestawienie stwierdzonych niezgodności z przypisaniem poziomu istotności oraz ryzyka;
(e) rekomendacje działań naprawczych wraz z proponowaną priorytetyzacją i szacunkową pracochłonnością;
(f) ocenę ogólną poziomu zgodności organizacji;
(g) streszczenie dla Kierownictwa (Executive Summary).

Format: dokument PDF (lub równoważny) spełniający wymagania dostępności cyfrowej oraz wersja edytowalna .docx (lub równoważna, np. .odt). Raport sporządza się w formie umożliwiającej bezpieczne udostępnienie organowi właściwemu do spraw cyberbezpieczeństwa, bez ujawniania szczegółów technicznych podatności mogących stanowić zagrożenie dla bezpieczeństwa Zamawiającego.

5. Warunki odbioru Pozycji 1.1

1) Odbiór następuje na podstawie Protokołu Odbioru Pozycji 1.1 podpisanego bez zastrzeżeń, po doręczeniu Raportu z Audytu Zgodności w wersji finalnej.
2) Zamawiający weryfikuje kompletność Raportu w terminie **1 dnia roboczego od dnia jego doręczenia** i albo podpisuje Protokół Odbioru, albo zgłasza pisemnie uwagi; Wykonawca usuwa uchybienia w terminie wyznaczonym przez Zamawiającego, **tak aby Protokół Odbioru Pozycji 1.1 oraz Protokół Odbioru Końcowego zostały podpisane nie później niż w dniu 29 grudnia 2026 r**.
3) Protokół Odbioru Końcowego podpisywany jest po odbiorze Pozycji 1.1**, nie później niż w dniu 29 grudnia 2026 r.**