OPIS PRZEDMIOTU ZAMÓWIENIA

Audyt SZBI na zgodność z KRI/UoKSC

Zapytanie Ofertowe nr 2/CW/0152/Świlcza – Część 1

1. Informacje ogólne

1.1. Zamawiający i odbiorca końcowy

Zamawiający	Gmina Świlcza, Świlcza 168, 36-072 Świlcza, NIP: 517-00-45-613, REGON: 690582140
Odbiorca końcowy (miejsce realizacji)	Zakład Wodociągów i Kanalizacji w Świlczy, Świlcza 168, 36-072 Świlcza, NIP: 813-001-27-38, REGON: 690227114 – samorządowy zakład budżetowy Gminy Świlcza nieposiadający osobowości prawnej (dalej: „Zakład”)
Adres do korespondencji	Świlcza 168, 36-072 Świlcza; e-mail: przetargi@swilcza.com.pl

1.2. Źródło finansowania

Program	Krajowy Plan Odbudowy i Zwiększania Odporności (KPO), środki Instrumentu na rzecz Odbudowy i Zwiększania Odporności – NextGenerationEU
Priorytet / inwestycja	C3 Cyberbezpieczeństwo / C3.1.1 Cyberbezpieczeństwo – CyberPL; konkurs grantowy „Cyberbezpieczne Wodociągi”, nabór KPOD.05.10-CW.01-001/25
Projekt	„Cyberbezpieczne wodociągi w Gminie Świlcza”, Umowa o powierzenie grantu nr KPOD.05.10-CW.01-001/25/0152/KPOD.05.10-CW.01-001/25/2026 z dnia 10.04.2026 r. (zmieniona Aneksem nr 1); kategoria kosztu U25 – Zadanie 1 „Obszar organizacyjny”

2. Przedmiot zamówienia

Przedmiotem zamówienia jest przeprowadzenie niezależnego audytu zgodności Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) wdrożonego w Zakładzie z wymaganiami rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności (KRI) oraz ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (UoKSC), wraz z opracowaniem Raportu z Audytu zawierającego ustalenia i rekomendacje działań korygujących. Audyt nie stanowi audytu bezpieczeństwa systemu informacyjnego, o którym mowa w art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Kody CPV: 79212000-3 Usługi audytu; 72810000-1 Usługi audytu komputerowego.

3. Kontekst i cel zamówienia

Zakład prowadzi zbiorowe zaopatrzenie w wodę i zbiorowe odprowadzanie ścieków na terenie Gminy Świlcza, wykorzystując infrastrukturę informatyczną (IT) oraz technologii operacyjnej (OT), w tym systemy sterowania i telemetrii obiektów technologicznych (stacje uzdatniania wody, ujęcia wody, oczyszczalnia ścieków, przepompownie).

W ramach Zadania 1 „Obszar organizacyjny” Projektu grantowego Zakład wdraża System Zarządzania Bezpieczeństwem Informacji (kategoria kosztu U20) zgodny z wymaganiami normy PN-EN ISO/IEC 27001:2023 (ISO/IEC 27001:2022), ustawy o krajowym systemie cyberbezpieczeństwa i dyrektywy NIS2, uwzględniający środowiska IT oraz OT/ICS/SCADA i obejmujący m.in. politykę bezpieczeństwa informacji, analizę ryzyka i plan postępowania z ryzykiem, procedury operacyjne, procedurę zarządzania incydentami oraz plan ciągłości działania. Dokumentacja SZBI jest opracowywana i wdrażana przez odrębnego wykonawcę w ramach zamówienia nr 1/CW/0152/Świlcza – Część 1, z terminem realizacji do 30.11.2026 r. W Urzędzie Gminy Świlcza funkcjonuje odrębny system zarządzania bezpieczeństwem informacji; SZBI Zakładu został opracowany z jego uwzględnieniem.

Celem zamówienia jest przeprowadzenie – zgodnie z Wnioskiem o przyznanie grantu – obiektywnej i niezależnej weryfikacji wdrożonego SZBI, tj. ustalenie, czy SZBI spełnia wymogi określone w rozporządzeniu KRI oraz w ustawie o krajowym systemie cyberbezpieczeństwa, w zakresie, w jakim mają one zastosowanie do Zakładu jako podmiotu

prowadzącego działalność w zakresie zbiorowego zaopatrzenia w wodę i zbiorowego odprowadzania ścieków, a także wskazanie ewentualnych niezgodności wraz z rekomendacjami działań korygujących.

Audyt służy w szczególności:

– uzyskaniu obiektywnych dowodów co do zgodności SZBI z kryteriami audytu wskazanymi w pkt 4;
– wypełnieniu obowiązku zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, o którym mowa w § 19 ust. 2 pkt 14 rozporządzenia KRI;
– zidentyfikowaniu niezgodności i obszarów wymagających doskonalenia, w szczególności w środowisku OT/ICS/SCADA objętym SZBI;
– dostarczeniu kierownictwu Zakładu i Zamawiającego rzetelnej podstawy do decyzji o dalszych działaniach w obszarze cyberbezpieczeństwa, w tym w okresie utrzymania SZBI (kategoria kosztu U21);
– udokumentowaniu wykonania pozycji budżetowej U25 na potrzeby rozliczenia Projektu grantowego i jego wskaźników.

4. Kryteria audytu

Audyt przeprowadza się wobec następujących kryteriów:

– rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2024 poz. 773) – § 19 ust. 1–3, w tym pełna weryfikacja realizacji działań wymienionych w § 19 ust. 2 pkt 1–14, a także § 20 (rozliczalność i dzienniki systemów);
– ustawa 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. – Dz.U. 2026 poz. 252) – w zakresie obowiązków Zakładu jako podmiotu krajowego systemu cyberbezpieczeństwa, w szczególności dotyczących środków zarządzania ryzykiem, obsługi i zgłaszania incydentów do właściwego CSIRT, korzystania z Systemu S46 oraz bezpieczeństwa łańcucha dostaw;
– wymagania rozdziałów 4–10 normy PN-EN ISO/IEC 27001:2023 oraz Deklaracja stosowania Zakładu (zabezpieczenia z Załącznika A) – w zakresie, w jakim SZBI Zakładu został na tej normie oparty;
– wewnętrzna dokumentacja SZBI Zakładu – zgodność praktyki organizacyjnej z treścią obowiązujących polityk, procedur i rejestrów;
– obowiązki przyjęte przez Zamawiającego w Umowie o powierzenie grantu oraz oświadczenia złożone we Wniosku o przyznanie grantu (m.in. objęcie zasobów teleinformatycznych monitoringiem serwisu moje.cert.pl i odbiór komunikatów bezpieczeństwa, korzystanie z Systemu S46, oświadczenie o wykorzystywaniu technologii operacyjnych oraz deklaracja implementacji wytycznych Komunikatu Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa w sprawie ataków na przemysłowe systemy sterowania ICS/OT).

Jako dokumenty odniesienia (dobre praktyki) stosuje się w szczególności normy PN-EN ISO/IEC 27002 i 27005, PN-EN ISO 22301, serię PN-EN IEC 62443 i NIST SP 800-82 (w odniesieniu do środowiska OT), dyrektywę NIS2 oraz Komunikat Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa w sprawie ataków na przemysłowe systemy sterowania (ICS/OT). Audyt prowadzony jest zgodnie z wytycznymi normy PN-EN ISO 19011 dotyczącymi audytowania systemów zarządzania.

Audyt prowadzi się według stanu prawnego obowiązującego na dzień zakończenia czynności audytowych. Wykonawca rozróżnia w ustaleniach obowiązki już obowiązujące Zakład, wymagania objęte okresami przejściowymi oraz zalecenia wynikające z dobrych praktyk, a przy każdej niezgodności wskazuje podstawę oceny.

5. Zakres audytu

Audytem objęte są wszystkie komórki organizacyjne Zakładu oraz oba środowiska teleinformatyczne:

– środowisko IT – systemy wspierające działalność administracyjną, obsługę klienta, rozliczenia, pocztę elektroniczną i obieg dokumentów, w tym rozwiązania bezpieczeństwa IT wdrażane w Projekcie grantowym (m.in. SIEM/SOAR, NAC, MDM, system kopii zapasowych);
– środowisko OT/ICS/SCADA – system monitoringu i sterowania pracą obiektów technologicznych w zakresie zaopatrzenia w wodę i odbioru ścieków, sterowniki i moduły telemetryczne, transmisja danych

telemetrycznych (sieć GSM/LTE z usługą Private APN, sieć LoRaWAN), stanowiska operatorskie SCADA oraz kanały zdalnego dostępu serwisowego.

Audyt obejmuje również styki SZBI Zakładu z systemem zarządzania bezpieczeństwem informacji Urzędu Gminy Świlcza (usługi i zasoby współdzielone, podział ról i odpowiedzialności) – w zakresie niezbędnym do oceny SZBI Zakładu, bez audytu systemu Urzędu Gminy.

Audyt obejmuje co najmniej następujące obszary:

- Organizacja bezpieczeństwa informacji – zakres SZBI, kontekst organizacji, zaangażowanie kierownictwa, przydział ról i odpowiedzialności, zasoby.
- Regulacje wewnętrzne i ich aktualność (§ 19 ust. 2 pkt 1 KRI) – kompletność, aktualność i spójność dokumentacji SZBI, jej formalne zatwierdzenie i zakomunikowanie.
- Inwentaryzacja sprzętu i oprogramowania (§ 19 ust. 2 pkt 2 KRI) – aktualność rejestru aktywów, w tym pokrycie aktywów OT.
- Zarządzanie ryzykiem (§ 19 ust. 2 pkt 3 KRI) – aktualność analizy ryzyka, adekwatność metodyki, kompletność planu postępowania z ryzykiem, uwzględnienie ryzyk środowiska OT.
- Zarządzanie uprawnieniami (§ 19 ust. 2 pkt 4 i 5 KRI) – nadawanie, przegląd i odbieranie uprawnień, konta uprzywilejowane i serwisowe, terminowość zmian przy zmianie zadań pracownika.
- Szkolenia i świadomość (§ 19 ust. 2 pkt 6 KRI) – realizacja szkoleń, ich zakres i udokumentowanie.
- Ochrona przetwarzanych informacji (§ 19 ust. 2 pkt 7 i 9 KRI) – monitorowanie dostępu, wykrywanie działań nieautoryzowanych, zabezpieczenia systemów operacyjnych, usług sieciowych i aplikacji.
- Praca zdalna i przetwarzanie mobilne (§ 19 ust. 2 pkt 8 KRI), w tym zarządzanie urządzeniami mobilnymi.
- Bezpieczeństwo łańcucha dostaw (§ 19 ust. 2 pkt 10 KRI) – klauzule bezpieczeństwa w umowach serwisowych, ocena ryzyka dostawców, weryfikacja dostawców wysokiego ryzyka.
- Bezpieczeństwo systemów teleinformatycznych (§ 19 ust. 2 pkt 12 KRI) – aktualizacje, kopie zapasowe i testy odtworzeń, ochrona przed utratą i nieuprawnioną modyfikacją, kryptografia, zarządzanie podatnościami.
- Zarządzanie incydentami (§ 19 ust. 2 pkt 13 KRI, UoKSC) – procedura, rejestr incydentów, znajomość ścieżki i terminów zgłoszeń, gotowość do korzystania z Systemu S46, monitoring moje.cert.pl.
- Audyt wewnętrzny i przegląd zarządzania (§ 19 ust. 2 pkt 14 KRI) – program audytów, przeglądy zarządzania, obieg działań korygujących.
- Rozliczalność i dzienniki systemów (§ 20 KRI) – zakres rejestrowanych zdarzeń, okres przechowywania, ochrona dzienników przed modyfikacją.
- Ciągłość działania – aktualność planów ciągłości działania i odtwarzania, udokumentowane testy, scenariusze dotyczące procesów technologicznych, w tym zasilania gwarantowanego i awaryjnego (UPS, mobilny agregat prądotwórczy) oraz strategia kopii zapasowych (3-2-1).
- Bezpieczeństwo środowiska OT/ICS/SCADA na poziomie systemu zarządzania – segmentacja IT/OT, zasady i nadzór nad zdalnym dostępem serwisowym, zarządzanie zmianą i aktualizacjami w OT, kopie konfiguracji i programów sterowników, bezpieczeństwo fizyczne obiektów rozproszonych, nośniki w środowisku OT oraz procedury eksploatacji zabezpieczeń OT wdrażanych w Projekcie grantowym (system IDS z sondami OT, przemysłowe routery z funkcją firewall, bramy LoRaWAN, Private APN, UPS dla sieci OT) – w tym zasady reagowania na alerty, kontroli dostępu zdalnego i zarządzania regułami komunikacji (bez testowania tych urządzeń).
- Ochrona danych osobowych w zakresie powiązanym z SZBI – spójność dokumentacji SZBI z dokumentacją ochrony danych, obieg zgłoszeń naruszeń.

Z zakresu audytu wyłączone są: audyt cyberbezpieczeństwa sieci OT (Część 2 zamówienia, pozycja budżetu U37), testy penetracyjne i aktywne skanowanie systemów, testy socjotechniczne oraz wdrażanie działań korygujących.

6. Wymagania wobec zespołu audytowego

Audyt prowadzi zespół Wykonawcy z udziałem co najmniej 1 (jednej) osoby pełniącej funkcję Audytora wiodącego, spełniającej wymagania określone w rozdziale „Osoby zdolne do wykonania zamówienia” Zapytania Ofertowego

(Część 1) i wskazanej w Wykazie osób (Załącznik nr 3 do ZO). W skład zespołu mogą wchodzić również inne osoby, działające pod kierunkiem Audytora wiodącego.

- Kluczowe czynności audytowe – planowanie, pozyskiwanie i ocena dowodów, formułowanie ustaleń oraz sporządzenie i podpisanie raportu – wykonuje lub nadzoruje osobiście Audytor wiodący, który uczestniczy w czynnościach audytowych na miejscu.
- Żaden członek zespołu audytowego nie może uczestniczyć w opracowaniu, wdrożeniu lub utrzymaniu audytowanej dokumentacji SZBI, w tym w ramach zamówienia na opracowanie i wdrożenie SZBI (kategoria kosztu U20, postępowanie nr 1/CW/0152/Świlcza – Część 1), ani pozostawać w stosunku pracy, zlecenia lub innym stosunku prawnym z wykonawcą tego zamówienia.
- Każdy członek zespołu audytowego składa oświadczenie o bezstronności i niezależności według wzoru stanowiącego Załącznik nr 1 do OPZ – przed rozpoczęciem czynności audytowych oraz ponownie jako załącznik do Raportu z Audytu.
- Wykonawca niezwłocznie informuje Zamawiającego o każdej okoliczności powstałej w toku realizacji umowy, która mogłaby wpłynąć na bezstronność lub niezależność audytu.

7. Metody audytowe i sposób realizacji

Audyt prowadzony jest metodami właściwymi dla audytu systemu zarządzania:

- przegląd dokumentacji i zapisów (dokumenty, rejestry, protokoły, logi w zakresie udostępnionym przez Zamawiającego);
- wywiady z kierownictwem Zakładu, właścicielami procesów, personelem IT oraz personelem obsługującym systemy OT – nie mniej niż 4 wywiady (w tym co najmniej 1 z kierownictwem Zakładu i co najmniej 1 z personelem obsługującym systemy OT);
- obserwacja procesów i oględziny obiektów – siedziba Zakładu oraz co najmniej 1 obiekt technologiczny wskazany przez Zamawiającego;
- weryfikacja próbek – dobór i sprawdzenie reprezentatywnych przypadków (np. nadania i odebrania uprawnień, obsługi zgłoszenia incydentu, sesji zdalnego dostępu serwisowego, odtworzenia z kopii zapasowej, oceny dostawcy).

Czynności audytowe na miejscu prowadzone są w siedzibie Zakładu: Świlcza 168, 36-072 Świlcza, oraz we wskazanym obiekcie technologicznym na terenie Gminy Świlcza. Wywiady, obserwacje, weryfikacja próbek i oględziny obiektów odbywają się na miejscu.

Zdalnie mogą być realizowane wyłącznie: przegląd dokumentacji przekazanej przez Zamawiającego, przygotowanie planu audytu, spotkanie otwierające oraz opracowanie raportu, a inne czynności – tylko za pisemną zgodą Zamawiającego na konkretny zakres prac.

Prace w obiektach technologicznych i w środowisku OT/ICS/SCADA podlegają następującym rygorom, przy czym naruszenie zakazu ingerencji w systemy produkcyjne lub zakazu skanowania aktywnego i prób uwierzytelniania (dwa pierwsze rygory poniżej) stanowi rażące naruszenie umowy, a za naruszenie pozostałych rygorów Wykonawca odpowiada na zasadach określonych we wzorze umowy:

- zakaz ingerencji w systemy produkcyjne – Wykonawca nie dokonuje jakichkolwiek zmian w sterownikach PLC/RTU, stacjach operatorskich SCADA, urządzeniach sieciowych ani innych elementach infrastruktury OT;
- zakaz skanowania aktywnego, prób uwierzytelniania i jakichkolwiek działań mogących zakłócić pracę systemów sterowania; odczyt konfiguracji z konsol zarządzających jest dopuszczalny wyłącznie za zgodą Zamawiającego i pod nadzorem jego personelu;
- wszystkie czynności w obiektach technicznych odbywają się w obecności wyznaczonego pracownika Zakładu;
- podłączanie do sieci Zakładu urządzeń lub nośników Wykonawcy wymaga uprzedniej zgody Zamawiającego, a nośniki muszą zostać uprzednio poddane kontroli antywirusowej;
- osoby wchodzące na teren obiektów technicznych stosują się do zasad BHP i wskazanych przez Zamawiającego środków ochrony indywidualnej;
- o każdym zdarzeniu mogącym mieć wpływ na ciągłość pracy systemów OT Wykonawca powiadamia Zamawiającego niezwłocznie, nie później niż w ciągu 1 godziny.

8. Plan realizacji i termin

Etap	Opis i termin
Czynności przygotowawcze	Od dnia zawarcia umowy: przygotowanie planu audytu i list kontrolnych, uzgodnienie spraw organizacyjnych, złożenie zobowiązań do zachowania poufności i oświadczeń o bezstronności.
Inicjalizacja	Po przekazaniu przez Zamawiającego dokumentacji SZBI: spotkanie otwierające (dopuszczalna forma zdalna), przedstawienie planu audytu (cele, kryteria, zakres, harmonogram, skład zespołu, wykaz dokumentów i osób) do akceptacji Zamawiającego.
Audyt dokumentacji	Przegląd dokumentacji SZBI wobec kryteriów audytu – po jej przekazaniu przez Zamawiającego (po odbiorze dokumentacji od wykonawcy wdrożenia SZBI).
Audyt na miejscu	Wywiady, obserwacje, weryfikacja próbek, oględziny – po odbiorze końcowym wdrożenia SZBI (planowo od 1 grudnia 2026 r.), w terminie uzgodnionym z Zamawiającym, nie krócej niż 2 dni robocze.
Spotkanie zamykające	Prezentacja wstępnych ustaleń dla kierownictwa Zakładu – w ostatnim dniu audytu na miejscu.
Raport wstępny	Przekazanie Raportu z Audytu w wersji roboczej – nie później niż do **14 grudnia 2026 r.**
Raport końcowy	Przekazanie Raportu w wersji finalnej po rozpatrzeniu uwag Zamawiającego – w terminie 1 dnia roboczego od ich otrzymania albo od upływu terminu na ich zgłoszenie.
Termin końcowy	Realizacja i odbiór całości (protokół odbioru) – nie później niż do **18 grudnia 2026 r.**

Zamawiający niezwłocznie zawiadamia Wykonawcę (drogą elektroniczną) o odbiorze dokumentacji SZBI i o odbiorze końcowym wdrożenia SZBI. Termin końcowy wynika z konieczności dokonania płatności przed końcem okresu kwalifikowalności wydatków Projektu grantowego (31 grudnia 2026 r.).

9. Klasyfikacja ustaleń audytowych

Kategoria	Definicja
Niezgodność główna (Major NC)	Brak realizacji wymagania stanowiącego kryterium audytu albo niezgodność systemowa powodująca, że dany element SZBI nie funkcjonuje; obejmuje w szczególności brak wymaganego dokumentu, brak realizacji obowiązku ustawowego lub brak dowodów wykonania działania wymaganego przepisem.
Niezgodność pomocnicza (Minor NC)	Pojedyncze odstępstwo od wymagania, niepowodujące niesprawności systemu jako całości.
Obserwacja (OBS)	Ustalenie wskazujące na ryzyko przekształcenia się w niezgodność, jeżeli nie zostaną podjęte działania.
Możliwość doskonalenia (OFI)	Rekomendacja podniesienia skuteczności lub efektywności rozwiązania spełniającego wymagania.

Każde ustalenie zawiera: opis stwierdzonego stanu, wskazanie wymagania (z dokładnym odwołaniem do przepisu, klauzuli normy albo dokumentu wewnętrznego), dowód (wskazanie dokumentu, zapisu, wypowiedzi lub obserwacji) oraz rekomendację działania korygującego.

10. Produkt – Raport z Audytu

Wykonawca dostarcza Raport z Audytu zawierający co najmniej:

- cel, zakres i kryteria audytu, skład zespołu audytowego wraz z posiadanymi certyfikatami oraz harmonogram czynności audytowych;
- metodykę audytu, wykaz przeglądanej dokumentacji, listę osób (funkcji), z którymi przeprowadzono wywiady, oraz wykaz obiektów objętych oględzinami;
- tabelaryczną ocenę zgodności z każdym z wymagań § 19 ust. 2 pkt 1–14 oraz § 20 rozporządzenia KRI (ZGODNY / CZĘŚCIOWO ZGODNY / NIEZGODNY) wraz z uzasadnieniem i wskazaniem dowodów;

- tabelaryczną ocenę zgodności z wymaganiami UoKSC objętymi zakresem audytu;
- ocenę zgodności z wymaganiami rozdziałów 4–10 normy PN-EN ISO/IEC 27001:2023 oraz ocenę kompletności i spójności dokumentacji SZBI, w tym analizy ryzyka, planu postępowania z ryzykiem i deklaracji stosowania;
- odrębny rozdział poświęcony środowisku OT/ICS/SCADA, obejmujący obszary wskazane w pkt 5;
- zestawienie wszystkich ustaleń (Major NC / Minor NC / OBS / OFI) z klasyfikacją, dowodami i rekomendacjami;
- plan działań korygujących z propozycją priorytetów, terminów i osób (funkcji) odpowiedzialnych, omówiony z Zamawiającym na etapie raportu wstępnego;
- ocenę ogólną poziomu zgodności SZBI z wymaganiami KRI i UoKSC;
- wnioski i rekomendacje dla kierownictwa (podsumowanie zarządcze);
- oświadczenia o bezstronności i niezależności, według wzoru stanowiącego Załącznik nr 1 do OPZ, podpisane przez każdego członka zespołu audytowego.

Raport sporządza się w formie umożliwiającej bezpieczne udostępnienie organom właściwym do spraw cyberbezpieczeństwa oraz podmiotom kontrolującym wydatki KPO, bez ujawniania szczegółów technicznych podatności mogących stanowić zagrożenie dla bezpieczeństwa Zakładu; szczegóły techniczne, jeżeli są niezbędne, umieszcza się w odrębnym, oznaczonym aneksie.

Raport przekazuje się w języku polskim, w formacie PDF podpisanym kwalifikowanym podpisem elektronicznym przez Audytora wiodącego, spełniającym wymagania dostępności cyfrowej (aktywna warstwa tekstowa, struktura nagłówków), oraz w wersji edytowalnej DOCX. Dokumenty oznacza się zestawieniem znaków: logo KPO, barwy Rzeczypospolitej Polskiej, znak Unii Europejskiej z napisem „Sfinansowane przez Unię Europejską – NextGenerationEU” oraz logo Centrum Projektów Polska Cyfrowa – zgodnie z Księgą Identyfikacji Wizualnej KPO.

11. Uwagi i warunki odbioru

- Wykonawca przekazuje Raport z Audytu w wersji roboczej osobie wyznaczonej przez Zamawiającego.
- Zamawiający zgłasza uwagi w terminie 2 dni roboczych od otrzymania raportu w wersji roboczej; uwagi mogą dotyczyć wyłącznie błędów faktycznych, kompletności opisu stanu faktycznego oraz formy raportu – nie mogą zmierzać do zmiany oceny audytora ani do usunięcia stwierdzonych niezgodności.
- Wykonawca przekazuje wersję finalną raportu wraz z odniesieniem się do każdej uwagi (uwzględniona / nieuwzględniona wraz z uzasadnieniem).
- Warunkiem podpisania protokołu odbioru jest: przeprowadzenie audytu na miejscu w zakresie określonym w pkt 7, przekazanie kompletnego Raportu z Audytu o zawartości zgodnej z pkt 10 oraz przekazanie podpisanych oświadczeń o bezstronności i niezależności.
- Zamawiający może odmówić odbioru raportu, który nie zawiera oceny zgodności z każdym z wymagań § 19 ust. 2 pkt 1–14 rozporządzenia KRI, nie zawiera odrębnego rozdziału dotyczącego środowiska OT albo w którym ustalenia nie zostały poparte wskazaniem dowodów.
- Stwierdzenie w raporcie niezgodności nie stanowi podstawy do odmowy odbioru ani do obniżenia wynagrodzenia Wykonawcy. Raport niezawierający jakichkolwiek ustaleń podlega weryfikacji Zamawiającego pod kątem rzetelności przeprowadzenia audytu.

12. Poufność i bezpieczeństwo informacji

- Wykonawca i wszystkie osoby zaangażowane w realizację zamówienia zachowują w ścisłej tajemnicy informacje uzyskane w toku audytu, w szczególności dane o infrastrukturze IT i OT/SCADA, wyniki analizy ryzyka, ustalenia audytowe i dokumenty wewnętrzne Zamawiającego i Zakładu – przez okres realizacji zamówienia oraz 5 lat po jego zakończeniu, a w odniesieniu do informacji, których ujawnienie mogłoby zagrozić bezpieczeństwu Zakładu – bezterminowo. Wykonawca zawiera umowy o zachowaniu poufności (NDA) ze wszystkimi osobami realizującymi audyt.
- Dokumentacja przekazywana jest uzgodnionym, szyfrowanym kanałem i przechowywana w postaci zaszyfrowanej, wyłącznie na terytorium Europejskiego Obszaru Gospodarczego; Wykonawca nie stosuje narzędzi pochodzących od dostawców uznanych za dostawców wysokiego ryzyka w rozumieniu UoKSC.
- Po odbiorze Wykonawca usuwa zbędne kopie danych Zamawiającego w terminie 30 dni, co potwierdza oświadczeniem, a Zamawiający cofa dostępy przyznane na potrzeby audytu. Przetwarzanie danych

osobowych w związku z audytem odbywa się na podstawie umowy powierzenia przetwarzania danych osobowych (Załącznik nr 7 do ZO).

13. Obowiązki Zamawiającego

- niezwłoczne przekazanie Wykonawcy dokumentacji SZBI po jej odbiorze oraz zawiadomienie o odbiorze końcowym wdrożenia SZBI i możliwości rozpoczęcia czynności na miejscu;
- wyznaczenie osoby do kontaktu oraz zapewnienie dostępności kierownictwa i personelu Zakładu (IT, OT, eksploatacja) w uzgodnionych terminach;
- zapewnienie dostępu do pomieszczeń i obiektów technologicznych oraz obecności wyznaczonego pracownika podczas czynności w obiektach.

14. Wymagania środowiskowe (zasada DNSH)

- Wykonawca realizuje przedmiot zamówienia zgodnie z zasadą „nie czyń poważnych szkód” (DNSH) w rozumieniu art. 5 ust. 2 rozporządzenia (UE) 2021/241 oraz art. 17 rozporządzenia (UE) 2020/852 oraz Wytycznymi technicznymi 2021/C 58/01, w tym nie podejmuje działań powodujących znaczącą szkodę dla celów środowiskowych;
- dokumenty, raporty i inne produkty audytu przekazywane są wyłącznie w postaci elektronicznej, a ich drukowanie ogranicza się do niezbędnego minimum;
- czynności, które zgodnie z pkt 7 mogą być realizowane zdalnie, Wykonawca realizuje w tej formie, ograniczając zbędne przemieszczanie się.

Załącznik nr 1 do OPZ – Oświadczenie członka zespołu audytowego o bezstronności i niezależności

Zamawiający	Gmina Świlcza, Świlcza 168, 36-072 Świlcza – odbiorca końcowy: Zakład Wodociągów i Kanalizacji w Świlczy
Zamówienie	Audyt SZBI na zgodność z KRI/UoKSC – Część 1 Zapytania Ofertowego nr 2/CW/0152/Świlcza
Wykonawca	……
Imię i nazwisko składającego oświadczenie	……
Rola w zespole audytowym	☐ Audytor wiodący ☐ Członek zespołu audytowego
Posiadany certyfikat uprawniający do przeprowadzenia audytu (dotyczy Audytora wiodącego)	nazwa: …… nr: …… ważny do: ……

Świadomy(-a) odpowiedzialności za złożenie oświadczenia niezgodnego z prawdą oświadczam, że:

- nie uczestniczyłem(-am) w opracowaniu, wdrożeniu, utrzymaniu ani aktualizacji dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji Zakładu podlegającej audytowi, w tym w ramach zamówienia nr 1/CW/0152/Świlcza – Część 1, i nie pozostaję w stosunku pracy, zlecenia ani w innym stosunku prawnym lub faktycznym z wykonawcą tego zamówienia ani z podmiotem należącym do tej samej grupy kapitałowej;
- nie wykonuję i w okresie roku przed rozpoczęciem audytu nie wykonywałem(-am) w Zakładzie zadań z zakresu zarządzania bezpieczeństwem systemów informacyjnych objętych audytem (w szczególności jako administrator, pełnomocnik ds. bezpieczeństwa informacji lub dostawca usług zarządzanych);
- nie pozostaję z Zamawiającym ani z osobami wykonującymi w jego imieniu czynności związane z realizacją zamówienia w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa lub powinowactwa w linii bocznej do drugiego stopnia, w stosunku przysposobienia, opieki lub kurateli ani we wspólnym pożyciu;
- nie posiadam interesu majątkowego ani osobistego w określonym wyniku audytu i nie zachodzą wobec mnie inne okoliczności mogące budzić uzasadnioną wątpliwość co do mojej bezstronności lub niezależności;
- zobowiązuję się przeprowadzić audyt rzetelnie, obiektywnie i wyłącznie na podstawie zebranych dowodów, zgodnie z kryteriami określonymi w Opisie Przedmiotu Zamówienia oraz z wytycznymi normy PN-EN ISO 19011;
- zobowiązuję się do zachowania w tajemnicy informacji uzyskanych w toku audytu, w szczególności o infrastrukturze IT i OT/SCADA Zakładu, stwierdzonych podatnościach i słabościach oraz danych osobowych;
- zobowiązuję się niezwłocznie poinformować Zamawiającego o każdej okoliczności, która mogłaby wpłynąć na moją bezstronność lub niezależność, i powstrzymać się od dalszych czynności audytowych do czasu rozstrzygnięcia sprawy przez Zamawiającego.

Oświadczenie składa każdy członek zespołu audytowego – przed rozpoczęciem czynności audytowych oraz ponownie jako załącznik do Raportu z Audytu.

……

(data i podpis składającego oświadczenie)