OPIS PRZEDMIOTU ZAMÓWIENIA

Audyt cyberbezpieczeństwa sieci OT

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

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 U37 – Zadanie 4 „Obszar techniczny OT”

2. Przedmiot zamówienia

Przedmiotem zamówienia jest przeprowadzenie niezależnego audytu cyberbezpieczeństwa sieci technologicznej OT (OT/ICS/SCADA) Zakładu, służącego – zgodnie z Wnioskiem o przyznanie grantu – identyfikacji zasobów, zmapowaniu komunikacji oraz wykryciu podatności w środowisku przemysłowym, a także ocenie poprawności implementacji i skuteczności zabezpieczeń sieci OT wdrażanych w Projekcie grantowym, wraz z opracowaniem Raportu z Audytu zawierającego ustalenia i rekomendacje działań naprawczych. 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: 72810000-1 Usługi audytu komputerowego; 79417000-0 Usługi doradcze w zakresie bezpieczeństwa; 79212000-3 Usługi audytu.

3. Kontekst i cel zamówienia

Zakład prowadzi zbiorowe zaopatrzenie w wodę i zbiorowe odprowadzanie ścieków na terenie Gminy Świlcza. Infrastruktura technologiczna obejmuje m.in. stacje uzdatniania wody, ujęcia wody, oczyszczalnię ścieków oraz przepompownie, nadzorowane przez system monitoringu i sterowania (SCADA) ze stanowiskami operatorskimi w siedzibie Zakładu, sterownikami z modułami telemetrycznymi w obiektach rozproszonych oraz transmisją danych w sieci komórkowej GSM/LTE.

W ramach Zadania 4 „Obszar techniczny OT” Projektu grantowego Zamawiający wdraża, w drodze odrębnego postępowania (nr RGI.271.22.2026), następujące zabezpieczenia i rozwiązania OT:

– system klasy IDS (Intrusion Detection System) dedykowany sieciom OT, realizujący pasywne monitorowanie sieci przemysłowej, automatyczną inwentaryzację urządzeń i mapowanie komunikacji;
– komplet 5 sprzętowych sond OT do analizy protokołów przemysłowych, współpracujących z systemem IDS;
– 4 przemysłowe routery z funkcją firewall klasy NGFW, przeznaczone do segmentacji i ochrony sieci OT na obiektach zdalnych (przepompownie, punkty ujęcia wody), z tunelami VPN do infrastruktury centralnej;

– 2 bramy LoRaWAN wraz z oprogramowaniem serwera sieciowego, do transmisji danych telemetrycznych z urządzeń końcowych;
– usługę wdrożenia rozwiązań w zakresie bezpieczeństwa OT (instalacja, konfiguracja i integracja ww. komponentów);
– urządzenia UPS do zabezpieczenia sieci OT, a w obszarze IT – m.in. usługę Private APN dla transmisji danych w sieci komórkowej oraz system kopii zapasowych.

Termin dostawy i wdrożenia ww. rozwiązań upływa nie później niż 15 grudnia 2026 r.; wdrożenia poszczególnych pozycji mogą być odbierane wcześniej.

Celem audytu jest w szczególności:

– identyfikacja i inwentaryzacja zasobów sieci OT (sterowniki i moduły telemetryczne, stanowiska operatorskie i serwery SCADA, urządzenia sieciowe) we wskazanych obiektach;
– zmapowanie komunikacji w sieci OT oraz na styku OT–IT i OT–Internet, w tym kanałów zdalnego dostępu serwisowego i transmisji telemetrycznej;
– wykrycie podatności, błędów konfiguracji i luk w zabezpieczeniach sieci OT, w tym ocena skuteczności segmentacji oraz konfiguracji zabezpieczeń wdrażanych w Projekcie grantowym;
– dostarczenie kierownictwu Zakładu rekomendacji działań naprawczych z priorytetami oraz udokumentowanie realizacji pozycji budżetowej U37 na potrzeby rozliczenia Projektu grantowego, w tym informacji do formularza potwierdzającego realną propozycję zwiększenia odporności (Załącznik nr 4 do Regulaminu Konkursu).

4. Dokumenty odniesienia

Audyt przeprowadza się z wykorzystaniem w szczególności następujących dokumentów odniesienia (lub dokumentów równoważnych, wskazanych przez Wykonawcę w planie audytu):

– seria norm PN-EN IEC 62443 (w szczególności IEC 62443-3-2 – ocena ryzyka, strefy i kanały oraz IEC 62443-3-3 – wymagania bezpieczeństwa systemu);
– NIST SP 800-82 Rev. 3 „Guide to Operational Technology (OT) Security”;
– Komunikat Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa w sprawie ataków na przemysłowe systemy sterowania (ICS/OT) oraz rekomendacje CSIRT dotyczące zabezpieczania systemów OT;
– ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. 2026 poz. 20 ze zm.) – w zakresie wymagań dotyczących bezpieczeństwa systemów informacyjnych;
– dokumentacja Zakładu, w tym dokumentacja SZBI (w zakresie dotyczącym OT) oraz dokumentacja powykonawcza zabezpieczeń OT wdrażanych w Projekcie grantowym.

Pomocniczo Wykonawca może stosować normy PN-EN ISO/IEC 27001 i 27002, CIS Benchmarks oraz NIST SP 800-115. Przyjętą metodykę Wykonawca wskazuje w planie audytu.

5. Zakres audytu

Audyt obejmuje sieć technologiczną OT Zakładu, w tym obiekty rozproszone, kanały transmisji danych (GSM/LTE, Private APN, LoRaWAN, tunele VPN), styk z siecią IT oraz kanały zdalnego dostępu, w co najmniej następujących obszarach:

1) Inwentaryzacja zasobów OT – identyfikacja urządzeń i systemów OT (sterowniki, moduły telemetryczne, HMI, stanowiska SCADA, serwery, urządzenia sieciowe, bramy LoRaWAN), z wykorzystaniem dokumentacji, oględzin i pasywnej analizy ruchu; weryfikacja kompletności i aktualności rejestru aktywów OT Zakładu.
2) Mapowanie komunikacji – identyfikacja przepływów OT–OT, OT–IT, OT–Internet i zdalnego dostępu, wykorzystywanych protokołów (w tym nieszyfrowanych protokołów przemysłowych) oraz połączeń nieautoryzowanych lub nieudokumentowanych.
3) Architektura i segmentacja – ocena podziału sieci na strefy i kanały komunikacji (zones & conduits), separacji sieci OT od sieci IT i Internetu oraz zgodności stanu faktycznego ze schematami sieci.
4) Konfiguracja zabezpieczeń wdrażanych w Projekcie grantowym – przegląd polityk i reguł filtrowania przemysłowych routerów z funkcją firewall (zasada najmniejszych uprawnień, reguły zbędne lub zbyt

szerokie), mechanizmów inspekcji protokołów przemysłowych, konfiguracji tuneli VPN i Private APN, konfiguracji systemu IDS i rozmieszczenia sond OT (pokrycie monitoringiem, reguły alarmowania, integracja z SIEM), konfiguracji bram i serwera LoRaWAN (uwierzytelnianie i szyfrowanie transmisji, zarządzanie kluczami), zarządzania urządzeniami i rejestrowania zdarzeń – wyłącznie w trybie odczytu, pod nadzorem Zamawiającego.

5) Zdalny dostęp i transmisja telemetryczna – ocena kanałów zdalnego dostępu serwisowego dostawców i integratorów (VPN, moduły i routery GSM/LTE, Private APN), uwierzytelniania, rejestrowania sesji i zarządzania kontami serwisowymi oraz pasywne rozpoznanie ekspozycji zasobów OT Zakładu w sieci Internet.
6) Hardening i podatności – ocena konfiguracji stanowisk operatorskich SCADA, serwerów i urządzeń sieciowych obszaru OT (konta i hasła domyślne, zbędne usługi, aktualizacje, ochrona przed złośliwym oprogramowaniem, kontrola nośników) w trybie odczytu oraz pasywna identyfikacja wersji oprogramowania i firmware'u wraz z korelacją z bazami podatności (CVE, ICS Advisories, komunikaty producentów).
7) Monitorowanie, kopie zapasowe i bezpieczeństwo fizyczne – ocena zdolności wykrywania incydentów w sieci OT (w tym wykorzystania systemu IDS oraz dzienników routerów z funkcją firewall), zakresu i retencji dzienników zdarzeń, synchronizacji czasu, kopii zapasowych konfiguracji i programów sterowników, oględziny zabezpieczeń fizycznych szaf i urządzeń w obiektach objętych oględzinami oraz ocena zasilania gwarantowanego urządzeń OT (UPS, agregat) w zakresie wpływu na dostępność.

Z zakresu audytu wyłączone są: aktywne skanowanie podatności i testy penetracyjne urządzeń automatyki (PLC/RTU, moduły telemetryczne, stanowiska SCADA), testy obciążeniowe i typu DoS, testy socjotechniczne, testy aplikacji internetowych, audyt SZBI na zgodność z KRI/UoKSC (Część 1 zamówienia, pozycja budżetu U25) oraz wdrażanie działań naprawczych. Weryfikacja reguł filtrowania na styku IT/OT może obejmować nieinwazyjne próby nawiązania połączenia wykonywane wyłącznie od strony sieci IT, w uzgodnionym oknie serwisowym i za uprzednią zgodą Zamawiającego.

6. Metody i minimalny zakres czynności na miejscu

Audyt prowadzony jest w szczególności następującymi metodami, w minimalnym zakresie:

Metoda	Minimalny zakres
Przegląd dokumentacji	Schematy sieci, rejestr aktywów, dokumentacja powykonawcza zabezpieczeń OT, procedury SZBI dotyczące OT.
Wywiady	Nie mniej niż 3 wywiady (kierownictwo Zakładu, osoby odpowiedzialne za eksploatację i automatykę, administrator IT; w miarę potrzeby – przedstawiciel serwisu systemu SCADA).
Oględziny obiektów	Nie mniej niż 2 obiekty technologiczne wskazane przez Zamawiającego (np. stacja uzdatniania wody oraz przepompownia lub oczyszczalnia ścieków, w tym co najmniej 1 obiekt wyposażony w router z funkcją firewall wdrażany w Projekcie, jeżeli został zainstalowany) oraz lokalizacja centralna (dyspozytornia / serwerownia w siedzibie Zakładu).
Pasywna analiza ruchu OT	Rejestracja ruchu w uzgodnionych punktach sieci OT – co najmniej w punkcie centralnym (port SPAN lub TAP) – przez okres nie krótszy niż 24 godziny, z wykorzystaniem urządzeń Wykonawcy pracujących wyłącznie w trybie pasywnym; jeżeli w danym punkcie rejestracja nie jest technicznie możliwa – za zgodą Zamawiającego analiza przechwytu ruchu lub danych z wdrożonego systemu IDS albo dzienników zdarzeń urządzeń sieciowych obejmujących co najmniej 24 godziny.
Przegląd konfiguracji	Odczyt lub eksport konfiguracji routerów z funkcją firewall, systemu IDS i sond, bram i serwera LoRaWAN, rozwiązań VPN/Private APN oraz wybranych urządzeń sieciowych i stanowisk SCADA – wyłącznie w trybie odczytu, przez personel Zamawiającego lub pod jego nadzorem.
Rozpoznanie ekspozycji	Pasywne rozpoznanie ekspozycji zasobów Zakładu w sieci Internet (np. publiczne wyszukiwarki urządzeń, informacje o adresacji publicznej).

Czynności na miejscu prowadzone są w siedzibie Zakładu (Świlcza 168, 36-072 Świlcza) oraz w obiektach technologicznych na terenie Gminy Świlcza. Zdalnie mogą być realizowane: przegląd dokumentacji i konfiguracji przekazanych przez Zamawiającego, analiza zarejestrowanego ruchu, przygotowanie planu audytu, spotkania otwierające i zamykające oraz opracowanie Raportu.

Zamawiający nie publikuje adresów obiektów ani przypisania urządzeń do obiektów, z uwagi na ochronę infrastruktury krytycznej. Wykaz obiektów objętych audytem wraz ze schematami sieci Zamawiający przekaże wybranemu Wykonawcy protokolarnie, w terminie 3 dni roboczych od dnia zawarcia umowy, po podpisaniu zobowiązania do zachowania poufności.

7. Rygory bezpieczeństwa prac w sieci OT

Prace w sieci OT i w obiektach technologicznych podlegają następującym rygorom, przy czym naruszenie rygorów określonych w pkt 1)–4) stanowi rażące naruszenie umowy, a za naruszenie pozostałych rygorów Wykonawca odpowiada na zasadach określonych we wzorze umowy:

1) czynności w sieci OT rozpoczynają się wyłącznie po akceptacji przez Zamawiającego planu audytu (zakres, metodyka, narzędzia, harmonogram, punkty rejestracji ruchu, zasady komunikacji i bezpiecznego przerwania prac); dopuszczalna jest akceptacja w formie elektronicznej;
2) zakaz ingerencji w systemy produkcyjne – Wykonawca nie dokonuje jakichkolwiek zmian w sterownikach, modułach telemetrycznych, stanowiskach SCADA, urządzeniach sieciowych ani innych elementach infrastruktury OT;
3) zakaz aktywnego skanowania urządzeń OT, prób uwierzytelniania, ataków siłowych oraz innych działań mogących zakłócić pracę systemów sterowania;
4) urządzenia rejestrujące ruch podłącza się wyłącznie w trybie pasywnym, za uprzednią zgodą Zamawiającego; nośniki i urządzenia Wykonawcy muszą zostać uprzednio poddane kontroli antywirusowej;
5) wszystkie czynności w obiektach i w sieci OT odbywają się w obecności wyznaczonego pracownika Zakładu; osoby wchodzące na teren obiektów stosują się do zasad BHP i wskazanych środków ochrony indywidualnej;
6) na żądanie Zamawiającego Wykonawca przerywa prace nie później niż w ciągu 15 minut; o każdym zdarzeniu mogącym mieć wpływ na ciągłość pracy systemów OT Wykonawca powiadamia Zamawiającego niezwłocznie, nie później niż w ciągu 1 godziny;
7) podatności krytyczne i wysokie oraz oznaki rzeczywistego naruszenia bezpieczeństwa Wykonawca zgłasza Zamawiającemu niezwłocznie, nie później niż w ciągu 24 godzin od ich stwierdzenia, nie czekając na Raport;
8) Wykonawca prowadzi rejestr wykonanych czynności (data i godzina, osoba, narzędzie, czynność, zasób) i przekazuje go Zamawiającemu jako załącznik do Raportu.

8. Zespół audytowy i niezależność

Audyt prowadzi zespół Wykonawcy z udziałem osób wskazanych w Wykazie osób (Załącznik nr 3 do ZO), spełniających wymagania określone w rozdziale „Osoby zdolne do wykonania zamówienia” Zapytania Ofertowego (Część 2) – Audytora wiodącego i Eksperta OT/ICS. Raport podpisuje Audytor wiodący.

– Ani Wykonawca, ani żaden członek zespołu audytowego nie może być podmiotem lub osobą, która dostarczała, wdrażała, konfigurowała lub utrzymuje w Zakładzie rozwiązania objęte audytem, w szczególności w ramach postępowania nr RGI.271.22.2026 (Część 3 „Dostawa rozwiązań OT”, w zakresie UPS dla sieci OT – Część 2, a w zakresie usługi Private APN – Część 1), ani podmiotem świadczącym na rzecz Zamawiającego serwis lub utrzymanie systemów sterowania, SCADA i telemetrii objętych audytem.
– Każdy członek zespołu audytowego składa oświadczenie o bezstronności i niezależności według wzoru stanowiącego Załącznik nr 1 do OPZ – przed rozpoczęciem czynności audytowych oraz jako załącznik do Raportu.

9. Harmonogram i termin realizacji

Audyt realizowany jest od dnia zawarcia umowy do dnia 23 grudnia 2026 r. Czynności niewymagające wdrożonych zabezpieczeń (Etap II) Wykonawca realizuje od zawarcia umowy, a weryfikację konfiguracji zabezpieczeń wdrażanych w Projekcie grantowym (Etap III) – po zawiadomieniu przez Zamawiającego o ich odbiorze. Audyt realizowany jest w następujących etapach:

Etap	Zakres
I. Inicjalizacja	Spotkanie otwierające (dopuszczalne zdalnie), przekazanie dokumentacji i wykazu obiektów, przedstawienie planu audytu do akceptacji, oświadczenia o bezstronności i zobowiązania do poufności.
II. Prace na miejscu i analiza ruchu	Wywiady, oględziny obiektów, rejestracja i analiza ruchu sieciowego OT, inwentaryzacja zasobów i mapowanie komunikacji, rozpoznanie ekspozycji, przegląd konfiguracji zabezpieczeń już odebranych przez Zamawiającego.
III. Weryfikacja konfiguracji wdrożonych zabezpieczeń	Przegląd konfiguracji zabezpieczeń OT (system IDS i sondy, routery z funkcją firewall, bramy i serwer LoRaWAN, VPN/Private APN) odebranych przez Zamawiającego po zakończeniu Etapu II – niezwłocznie po zawiadomieniu Wykonawcy o odbiorze wdrożenia (dopuszczalne zdalnie, na podstawie eksportów konfiguracji).
IV. Raport wstępny i spotkanie zamykające	Przekazanie Raportu w wersji roboczej – nie później niż do **21 grudnia 2026 r.** – i prezentacja ustaleń kierownictwu Zakładu (dopuszczalne zdalnie).
V. Raport końcowy i odbiór	Przekazanie Raportu w wersji finalnej po rozpatrzeniu uwag Zamawiającego, podpisanie protokołu odbioru – nie później niż do **23 grudnia 2026 r.**

Jeżeli którykolwiek z elementów zabezpieczeń wdrażanych w Projekcie grantowym nie zostanie odebrany przez Zamawiającego do dnia 15 grudnia 2026 r., audyt obejmuje stan faktyczny na dzień prowadzenia czynności, a Wykonawca odnotowuje w Raporcie elementy niewdrożone lub nieodebrane.

Termin końcowy wynika z konieczności rozliczenia wydatku przed końcem okresu kwalifikowalności wydatków Projektu grantowego (31 grudnia 2026 r.).

10. Klasyfikacja ustaleń

Kategoria	Definicja
Krytyczne	Podatność lub brak zabezpieczenia umożliwiający bezpośrednie przejęcie kontroli nad procesem technologicznym lub zakłócenie ciągłości dostaw wody / odbioru ścieków, w szczególności dostępny z Internetu lub z sieci IT bez skutecznej kontroli.
Wysokie	Istotna słabość zabezpieczeń, której wykorzystanie wymaga dodatkowych warunków, ale może prowadzić do naruszenia integralności lub dostępności systemów OT.
Średnie	Słabość ograniczająca skuteczność zabezpieczeń lub wykrywania, bez bezpośredniego wpływu na proces technologiczny.
Niskie / informacyjne	Odstępstwo od dobrych praktyk lub rekomendacja podniesienia poziomu bezpieczeństwa.

Każde ustalenie zawiera: opis stanu faktycznego, wymaganie lub dobrą praktykę (z odwołaniem do dokumentu odniesienia), dowód (dokument, zapis konfiguracji, fragment analizy ruchu lub obserwacja), ocenę ryzyka (dla podatności – z wykorzystaniem skali CVSS, o ile ma zastosowanie) oraz rekomendację działania naprawczego z priorytetem.

11. Produkt – Raport z Audytu

Wykonawca dostarcza Raport z Audytu zawierający co najmniej:

1) cel, zakres, kryteria i metodykę audytu, skład zespołu audytowego z posiadanymi certyfikatami oraz harmonogram czynności;
2) wykaz przeglądanej dokumentacji i konfiguracji, listę osób (funkcji), z którymi przeprowadzono wywiady, wykaz obiektów objętych oględzinami oraz opis punktów i okresu rejestracji ruchu;
3) wykaz zidentyfikowanych zasobów OT oraz aktualny schemat logiczny sieci OT z podziałem na strefy i kanały komunikacji;
4) macierz zaobserwowanych przepływów komunikacyjnych (OT–OT, OT–IT, OT–Internet, zdalny dostęp, telemetria) z oceną ich zasadności;

5) ocenę stanu zabezpieczeń w każdym z obszarów wskazanych w pkt 5, w tym ocenę konfiguracji systemu IDS i sond, routerów z funkcją firewall, bram i serwera LoRaWAN oraz VPN/Private APN, a także ocenę realizacji wytycznych Komunikatu Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa w sprawie ataków na przemysłowe systemy sterowania (ICS/OT);
6) zestawienie wszystkich ustaleń z klasyfikacją wg pkt 10, dowodami i rekomendacjami oraz plan działań naprawczych z proponowanymi priorytetami i terminami;
7) ocenę ogólną poziomu cyberbezpieczeństwa sieci OT oraz podsumowanie dla kierownictwa, zawierające zestawienie zabezpieczeń OT wdrożonych w Projekcie grantowym z oceną ich wdrożenia i skuteczności (do wykorzystania przy sporządzaniu formularza, o którym mowa w Załączniku nr 4 do Regulaminu Konkursu);
8) rejestr wykonanych czynności, potwierdzenie usunięcia narzędzi i danych tymczasowych oraz podpisane oświadczenia o bezstronności i niezależności.

Szczegóły techniczne podatności mogące stanowić zagrożenie dla bezpieczeństwa Zakładu umieszcza się w odrębnym, oznaczonym aneksie, tak aby część główną Raportu można było udostępnić podmiotom kontrolującym wydatki KPO.

Raport przekazuje się w języku polskim, w formacie PDF podpisanym kwalifikowanym podpisem elektronicznym oraz w wersji edytowalnej (DOCX); wykaz zasobów, macierz przepływów i zestawienie ustaleń – dodatkowo w formacie XLSX. Dokumenty oznacza się zestawieniem znaków KPO (logo KPO, barwy RP, znak UE z napisem „Sfinansowane przez Unię Europejską – NextGenerationEU", logo CPPC), zgodnie z Księgą Identyfikacji Wizualnej KPO.

12. Odbiór

– Zamawiający zgłasza uwagi do Raportu w wersji roboczej niezwłocznie, nie później niż w terminie 1 dnia roboczego od jego otrzymania; uwagi mogą dotyczyć wyłącznie błędów faktycznych, kompletności opisu stanu faktycznego oraz formy Raportu i nie mogą zmierzać do zmiany ocen audytora ani usunięcia ustaleń.
– Wykonawca przekazuje wersję finalną Raportu wraz z odniesieniem się do każdej uwagi (uwzględniona / nieuwzględniona z uzasadnieniem).
– Warunkiem podpisania protokołu odbioru jest przeprowadzenie czynności na miejscu w zakresie określonym w pkt 6 oraz przekazanie kompletnego Raportu o zawartości zgodnej z pkt 11.
– Stwierdzenie w Raporcie podatności lub niezgodności nie stanowi podstawy do odmowy odbioru ani do obniżenia wynagrodzenia.

13. Poufność i bezpieczeństwo informacji

– Wykonawca i osoby realizujące audyt zachowują w tajemnicy informacje uzyskane w toku audytu, w szczególności dane o infrastrukturze IT i OT/SCADA, konfiguracje, zarejestrowany ruch sieciowy i ustalenia audytowe – w okresie realizacji umowy oraz przez 5 lat po jej zakończeniu, a w zakresie informacji, których ujawnienie mogłoby zagrozić bezpieczeństwu Zakładu – bez ograniczenia w czasie.
– Dokumentacja, konfiguracje i zapisy ruchu przekazywane są uzgodnionym, szyfrowanym kanałem i przechowywane w postaci zaszyfrowanej, wyłącznie na terytorium Europejskiego Obszaru Gospodarczego; Wykonawca nie stosuje narzędzi dostawców uznanych za dostawców wysokiego ryzyka w rozumieniu ustawy o KSC.
– Po odbiorze Wykonawca usuwa z infrastruktury Zakładu swoje narzędzia i urządzenia, a pozyskane dane (w tym zapisy ruchu i konfiguracje) usuwa w terminie 30 dni, co potwierdza oświadczeniem. Przetwarzanie danych osobowych w związku z audytem odbywa się na podstawie umowy powierzenia przetwarzania danych osobowych (Załącznik nr 7 do ZO).

14. Obowiązki Zamawiającego

– przekazanie dokumentacji, schematów sieci i wykazu obiektów (w terminie, o którym mowa w pkt 6) oraz niezwłoczne zawiadamianie Wykonawcy o odbiorze wdrożeń zabezpieczeń OT;
– wyznaczenie osoby do kontaktu oraz zapewnienie dostępności kierownictwa i personelu Zakładu (IT, automatyka, eksploatacja) w uzgodnionych terminach;

– zapewnienie dostępu do obiektów, punktów rejestracji ruchu uzgodnionych w planie audytu oraz obecności wyznaczonego pracownika podczas czynności w obiektach i w sieci OT.

15. 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; w szczególności dokumenty przekazuje wyłącznie w postaci elektronicznej, a czynności, które mogą być realizowane zdalnie, 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 cyberbezpieczeństwa sieci OT – Zapytanie Ofertowe nr 2/CW/0152/Świlcza – Część 2
Wykonawca	……
Imię i nazwisko	……
Rola w zespole	☐ Audytor wiodący ☐ Ekspert OT/ICS ☐ Członek zespołu audytowego
Posiadany certyfikat	nazwa: …… nr: …… ważny do: ……

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

1) nie uczestniczyłem(-am) w dostawie, wdrożeniu, konfiguracji ani utrzymaniu w Zakładzie rozwiązań objętych audytem, w tym w ramach postępowania nr RGI.271.22.2026, i nie pozostaję w stosunku pracy, zlecenia ani w innym stosunku prawnym lub faktycznym z wykonawcami tych rozwiązań ani z podmiotami świadczącymi na rzecz Zamawiającego serwis systemów sterowania i telemetrii;
2) 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;
3) 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;
4) zobowiązuję się przeprowadzić audyt rzetelnie i obiektywnie, wyłącznie na podstawie zebranych dowodów, zgodnie z OPZ i zaakceptowanym planem audytu, oraz zachować w tajemnicy informacje uzyskane w toku audytu;
5) zobowiązuję się niezwłocznie poinformować Zamawiającego o każdej okoliczności mogącej wpłynąć na moją bezstronność i powstrzymać się od dalszych czynności audytowych do czasu rozstrzygnięcia sprawy przez Zamawiającego.

……
(data i podpis składającego oświadczenie)