ZAMAWIAJĄCY:

Gminna Spółka Komunalna Sp. z o.o. z siedzibą w Kamieniu Małym
Kamień Mały 4B, 14-200 Iława

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

na potrzeby postępowania pn. „Wzmocnienie systemu cyberbezpieczeństwa w Gminnej Spółce Komunalnej Sp. z o.o. z siedzibą w Kamieniu Małym w zakresie usług audytowych, testów bezpieczeństwa, usług doradczych i szkoleniowych”, realizowanego w ramach projektu „Cyberbezpieczne Wodociągi”, Inwestycja C3.1.1 „Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo”, Krajowy Plan Odbudowy i Zwiększania Odporności, finansowanego ze środków Instrumentu na rzecz Odbudowy i Zwiększania Odporności.

Spis treści

CZĘŚĆ WSTĘPNA
1. Przedmiot zamówienia i podział na zadania
2. Charakterystyka środowiska Zamawiającego
3. Wymagania ogólne
4. Kolejność realizacji i współdziałanie Wykonawców
5. Poufność, dostęp do infrastruktury i ochrona danych
6. Odbiory

ZADANIE NR 1 – AUDYTY I TESTY BEZPIECZEŃSTWA
1.A. Audyt początkowy
1.B. Audyt cyberbezpieczeństwa sieci IT/OT/ICS
1.C. Testy bezpieczeństwa (testy penetracyjne) IT i OT
1.D. Szkolenie powiązane z testami socjotechnicznymi
1.E. Audyt końcowy
1.F. Wymagania wobec sposobu realizacji Zadania nr 1

ZADANIE NR 2 – OPRACOWANIE I WDROŻENIE SZBI I SZCD WRAZ ZE SZKOLENIAMI
2.A–2.B. Opracowanie i wdrożenie SZBI i SZCD
2.C. Plany ciągłości działania (BCP) i odtwarzania po awarii (DRP)
2.D. Utrzymanie i doskonalenie SZBI
2.E. Doradztwo w zakresie warunków umów z dostawcami
2.F. Podstawowe szkolenie z zakresu cyberbezpieczeństwa dla pracowników
2.G. Szkolenie specjalistyczne dla kadry zarządzającej i pracowników IT
2.H. Szkolenie symulacyjne
2.I. Certyfikacja kompetencji osób
2.J. Wymagania wobec sposobu realizacji Zadania nr 2

CZĘŚĆ WSTĘPNA

1. Przedmiot zamówienia i podział na zadania

1. Przedmiotem zamówienia są usługi służące podniesieniu poziomu bezpieczeństwa informacji, cyberbezpieczeństwa i ciągłości działania Zamawiającego, podzielone na dwa zadania:

Zadanie	Zakres
Zadanie nr 1 – Audyty i testy bezpieczeństwa	1.A. Audyt początkowy SZBI i SZCD z oceną zgodności (KRI, uKSC); 1.B. Audyt cyberbezpieczeństwa sieci IT/OT/ICS; 1.C. Testy bezpieczeństwa (testy penetracyjne) IT i OT; 1.D. Szkolenie powiązane z testami socjotechnicznymi; 1.E. Audyt końcowy SZBI i SZCD z oceną zgodności
Zadanie nr 2 – SZBI i SZCD ze szkoleniami	2.A. Opracowanie i wdrożenie SZBI; 2.B. Opracowanie i wdrożenie SZCD; 2.C. Plany BCP i DRP; 2.D. Utrzymanie i doskonalenie SZBI; 2.E. Doradztwo w zakresie warunków umów z dostawcami; 2.F. Podstawowe szkolenie pracowników; 2.G. Szkolenie specjalistyczne dla kadry zarządzającej i IT; 2.H. Szkolenie symulacyjne; 2.I. Certyfikacja kompetencji osób

2. **Zasada niezależności.** Zadanie nr 1 obejmuje czynności weryfikujące, a Zadanie nr 2 – czynności wdrożeniowe. Zgodnie z PN-EN ISO 19011 i pkt 9.2 PN-EN ISO/IEC 27001 audytor nie powinien oceniać obszaru, za który sam odpowiada. Dlatego zadania realizują różni Wykonawcy, a ten sam podmiot ani ta sama osoba nie mogą uczestniczyć w realizacji obu zadań (Rozdział III ust. 5–6 i Rozdział VII ust. 5 SWP). Rozdzielenie zapewnia wiarygodność audytu końcowego i testów jako potwierdzenia efektów projektu.
3. Każdy element wskazany w tabeli stanowi odrębną pozycję Formularza cenowego (Załącznik nr 4 do SWP) i podlega odrębnemu odbiorowi częściowemu.

2. Charakterystyka środowiska Zamawiającego

Poniższe dane służą przygotowaniu porównywalnych ofert. Szczegółowe informacje o konfiguracji systemów, adresacji i zabezpieczeniach zostaną przekazane wybranemu Wykonawcy po zawarciu umowy i podpisaniu zobowiązania do zachowania poufności.

Parametr	Wartość
Liczba pracowników ogółem	19
w tym pracownicy IT / osoby odpowiedzialne za systemy IT i OT	2
Lokalizacje objęte zamówieniem	siedziba – Kamień Mały 4B, 14-200 Iława, oraz 121 obiektów technologicznych: 9 stacji uzdatniania wody, 18 ujęć wody i 94 przepompownie z telemetrią (Zamawiający nie eksploatuje oczyszczalni ścieków). Czynności na miejscu w obiektach technologicznych obejmują próbę obiektów określoną w pkt 1.B. Adresy obiektów zostaną przekazane wybranemu Wykonawcy po zawarciu umowy

Parametr	Wartość
Stanowiska komputerowe (szacunkowo)	7 stacji roboczych; łącznie ok. 21 urządzeń w sieci biurowej (komputery, drukarki, serwer, urządzenia sieciowe)
Serwery fizyczne / maszyny wirtualne	1; w ramach części technicznej projektu – serwer fizyczny dla rozwiązań bezpieczeństwa (w tym usług wysokiej dostępności) oraz macierz dyskowa
Systemy OT (SCADA, telemetria, sterowniki)	system SCADA z telemetrią obiektów, serwisowany przez firmę zewnętrzną; testy wyłącznie metodami nieinwazyjnymi (pkt 1.C ust. 3)
Publiczne adresy IP do testów zewnętrznych	do 2 adresów IP
Serwisy WWW do audytu	2 – strona internetowa gsk.ilawa.pl oraz elektroniczne biuro obsługi klienta ebok.gsk.ilawa.pl (utrzymywane przez podmiot zewnętrzny); testy serwisów utrzymywanych przez podmioty zewnętrzne Wykonawca prowadzi po uzyskaniu przez Zamawiającego zgody tych podmiotów
Domeny pocztowe do audytu	1 (gmina-ilawa.pl) – z zastrzeżeniem zgody właściciela domeny (poniżej tabeli)
Istniejąca dokumentacja bezpieczeństwa	brak wdrożonych systemów zabezpieczeń i sformalizowanej dokumentacji bezpieczeństwa informacji i ciągłości działania; dotychczasowe szkolenia obejmowały wyłącznie ochronę danych osobowych (zgodnie z wnioskiem o przyznanie grantu)
Status na gruncie uKSC	do ustalenia w ramach audytu początkowego (pkt 1.A ppkt 6)

Wartości wskazane w tabeli są szacunkowe i służą przygotowaniu porównywalnych ofert. Wykonawca uwzględnia w cenie ryczałtowej zakres faktycznie występujący u Zamawiającego, jeżeli nie przekracza on wartości wskazanych w tabeli o więcej niż 20%. Przekroczenie w tym zakresie nie stanowi podstawy do zmiany wynagrodzenia ani terminów realizacji.

W ramach odrębnego zamówienia (część techniczna projektu) Zamawiający planuje wdrożenie m.in.: systemu klasy SIEM, systemu klasy SOAR, oprogramowania klasy XDR, oprogramowania do zarządzania podatnościami i do badania podatności, oprogramowania do monitorowania infrastruktury informatycznej, oprogramowania klasy BAS, oprogramowania do ochrony przed ransomware, oprogramowania do zarządzania tożsamością i dostępem w środowisku OT, serwera fizycznego i macierzy dyskowej, a także usług SOC/MDR, CTI, inwentaryzacji aktywów teleinformatycznych oraz konfiguracji i hardeningu systemów. Zamawiający planuje zakończenie tych wdrożeń do dnia 18.12.2026 r.; umowa na ich realizację nie została jeszcze zawarta. Realizacja niniejszego zamówienia nie jest uzależniona od zakończenia części technicznej projektu: czynności Wykonawców obejmują infrastrukturę w stanie na dzień ich wykonania, w tym

rozwiązania wdrożone do tego dnia, a w zakresie rozwiązań jeszcze niewdrożonych – ich planowaną architekturę i założenia, na podstawie informacji przekazanych przez Zamawiającego.

Poczta elektroniczna Zamawiającego działa w domenie gmina-ilawa.pl, której właścicielem jest Gmina Iława. Czynności audytowe i testy dotyczące zasobów współdzielonych z Gminą Iława (w szczególności domeny i poczty elektronicznej) Wykonawca prowadzi wyłącznie w zakresie objętym pisemną zgodą właściciela tych zasobów, przekazaną przez Zamawiającego przed rozpoczęciem czynności.

3. Wymagania ogólne

1. Wykonawca wykonuje usługi z należytą starannością, zgodnie z aktualnym stanem wiedzy oraz przepisami prawa, normami i dobrymi praktykami obowiązującymi na dzień odbioru.
2. Rezultaty usług (raporty, dokumentacja, polityki, procedury, analizy, materiały szkoleniowe) muszą być kompletne, wzajemnie spójne, dostosowane do warunków Zamawiającego oraz wolne od wad fizycznych i prawnych. Wadą jest również niezgodność rezultatu z OPZ.
3. Rezultaty Wykonawca dostarcza w języku polskim, w wersji elektronicznej edytowalnej (DOCX/XLSX) oraz w wersji PDF podpisanej kwalifikowanym podpisem elektronicznym przez osoby wskazane w OPZ, a raporty z audytów i testów – dodatkowo w 1 egzemplarzu papierowym.
4. Wykonawca przenosi na Zamawiającego autorskie prawa majątkowe do rezultatów na polach eksploatacji określonych we Wzorze umowy, w tym prawo do ich modyfikowania i aktualizowania na potrzeby własne Zamawiającego.
5. Wskazanie norm, w tym Polskich Norm i norm ISO/IEC, oznacza dopuszczenie rozwiązań równoważnych, zapewniających spełnienie wymagań na poziomie nie niższym niż określony w przywołanej normie. Dopuszcza się stosowanie aktualnych wydań norm.
6. Wymagania OPZ są wymaganiami minimalnymi, chyba że z ich treści wynika inaczej.

4. Kolejność realizacji i współdziałanie Wykonawców

Zadania realizowane są w następującej kolejności:

Etap	Czynność	Termin
1	Zadanie nr 1 – audyt początkowy (1.A)	do 5 dni od zawarcia umowy, nie później niż do 14.12.2026 r.
2	Zadanie nr 2 – doradztwo w zakresie warunków umów (2.E)	od zawarcia umowy, nie później niż do 18.12.2026 r.
3	Przekazanie raportu z audytu początkowego Wykonawcy Zadania nr 2 – przez Zamawiającego	niezwłocznie po odbiorze, nie później niż w 1 dzień roboczy
4	Zadanie nr 2 – opracowanie, zatwierdzenie i wdrożenie SZBI i SZCD oraz planów BCP i DRP (2.A–2.C)	od zawarcia umowy, na podstawie analizy stanu wyjściowego, z

Etap	Czynność	Termin
		uwzględnieniem raportu z audytu początkowego po jego przekazaniu; przedłożenie do zatwierdzenia nie później niż do 17.12.2026 r.
5	Zadanie nr 1 – audyt sieci i testy bezpieczeństwa (1.B i 1.C)	od zawarcia umowy, równolegle z audytem początkowym, nie później niż do 18.12.2026 r.
6	Zadanie nr 1 – testy socjotechniczne ze szkoleniem (1.D)	po zatwierdzeniu dokumentacji SZBI (2.A), nie później niż do 21.12.2026 r.
7	Zadanie nr 2 – szkolenie podstawowe, specjalistyczne i symulacyjne (2.F, 2.G i 2.H)	po zatwierdzeniu 2.A–2.C, nie później niż do 21.12.2026 r.
8	Zadanie nr 2 – utrzymanie i doskonalenie SZBI (2.D)	od zatwierdzenia dokumentacji SZBI do 22.12.2026 r.
9	Zadanie nr 2 – certyfikacja kompetencji osób (2.I)	egzamin nie później niż do 22.12.2026 r.
10	Zadanie nr 1 – audyt końcowy (1.E), z uwzględnieniem wyników 1.B–1.D i dokumentacji SZBI i SZCD	po odbiorze 1.B, 1.C i 2.A–2.C, nie później niż do 22.12.2026 r.

1. Całość zamówienia musi zostać zrealizowana i odebrana w okresie kwalifikowalności wydatków projektu, nie później niż do dnia 22.12.2026 r. (wykonanie i odbiór wszystkich elementów obu zadań).
2. Wykonawcy obu zadań nie kontaktują się ze sobą bezpośrednio w sprawach merytorycznych. Przekazywanie informacji między zadaniami odbywa się za pośrednictwem Zamawiającego.
3. Zasady zmiany terminów w razie opóźnienia w drugim zadaniu albo udostępnienia materiałów lub środowiska przez Zamawiającego określają Wzory umów.

5. Poufność, dostęp do infrastruktury i ochrona danych

1. Informacje o infrastrukturze, konfiguracji, podatnościach i zabezpieczeniach Zamawiającego stanowią informacje poufne. Przed rozpoczęciem prac każda osoba skierowana do realizacji zamówienia podpisuje zobowiązanie do zachowania poufności.
2. Dostęp do systemów, w tym dostęp zdalny, odbywa się wyłącznie w sposób uzgodniony z Zamawiającym, z imienną identyfikacją osób i – w miarę możliwości technicznych – rejestracją czynności.
3. Jeżeli realizacja zamówienia wymaga przetwarzania danych osobowych w imieniu Zamawiającego (w szczególności danych zawartych w dokumentacji audytowanej lub przekazywanych na potrzeby szkoleń), strony zawierają umowę powierzenia przetwarzania danych zgodnie z art. 28 RODO przed rozpoczęciem przetwarzania.

4. Po zakończeniu realizacji Wykonawca zwraca lub trwale usuwa informacje poufne, w tym dane z testów, i składa oświadczenie o ich usunięciu.

6. Odbiory

1. Każdy element zadania (pozycja Formularza cenowego) podlega odbiorowi częściowemu potwierdzonemu protokołem.
2. Zamawiający zgłasza uwagi do przedłożonego rezultatu w terminie 2 dni roboczych od jego otrzymania. Wykonawca uwzględnia uwagi i przedkłada poprawiony rezultat w terminie 2 dni roboczych.
3. Szczegółowe zasady odbiorów, płatności i odpowiedzialności określają Wzory umów.

ZADANIE NR 1 – AUDYTY I TESTY BEZPIECZEŃSTWA

1.A. Audyt początkowy

Przedmiotem usługi jest audyt początkowy obejmujący:

1. audyt Systemu Zarządzania Bezpieczeństwem Informacji (SZBI),
2. audyt Systemu Zarządzania Ciągłością Działania (SZCD),
3. ocenę zgodności organizacyjnej, technicznej, proceduralnej i formalnoprawnej Zamawiającego z wymaganiami dotyczącymi bezpieczeństwa informacji, cyberbezpieczeństwa i odporności operacyjnej.

Audyt służy ustaleniu stanu wyjściowego bezpieczeństwa organizacji, identyfikacji luk, podatności oraz braków organizacyjnych i proceduralnych, a także określeniu rekomendowanych działań naprawczych i wdrożeniowych. **Audyt musi zostać przeprowadzony przed opracowaniem dokumentacji SZBI i SZCD w Zadaniu nr 2**, ponieważ jego wyniki są podstawą tej dokumentacji. Audyt obejmuje stan na dzień jego przeprowadzenia, z uwzględnieniem rozwiązań wdrażanych w ramach części technicznej projektu – w zakresie, w jakim zostały już uruchomione.

Zakres audytu musi uwzględniać specyfikę przedsiębiorstwa wodociągowo-kanalizacyjnego, w tym środowisk IT i OT, systemów sterowania, automatyki przemysłowej, telemetrii, systemów SCADA, zdalnego monitoringu oraz infrastruktury istotnej dla ciągłości zbiorowego zaopatrzenia w wodę i odprowadzania ścieków.

Audyt przeprowadza się w oparciu o aktualnie obowiązujące przepisy prawa, normy, wytyczne i dobre praktyki, w szczególności:

– 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. z 2024 r. poz. 773) – dalej: „KRI”;

– ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20), z uwzględnieniem zmian wprowadzonych ustawą z dnia 23 stycznia 2026 r. (Dz. U. z 2026 r. poz. 252) – dalej: „uKSC”, wraz z aktami wykonawczymi;

– dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. (NIS2) – jako punkt odniesienia dla oceny dojrzałości w zakresie zarządzania ryzykiem cyberbezpieczeństwa, obsługi incydentów, ciągłości działania, bezpieczeństwa łańcucha dostaw, polityk, procedur, testowania i nadzoru;

– PN-EN ISO/IEC 27001 – wymagania dla systemu zarządzania bezpieczeństwem informacji;

– PN-EN ISO/IEC 27002 – zabezpieczenia bezpieczeństwa informacji;

– PN-EN ISO/IEC 27005 – zarządzanie ryzykiem w bezpieczeństwie informacji;

– PN-EN ISO 22301 – wymagania dla systemu zarządzania ciągłością działania;

– PN-EN ISO 22313 – wytyczne do wdrażania systemu zarządzania ciągłością działania;

– PN-EN ISO 19011 – wytyczne dotyczące auditowania systemów zarządzania;

– aktualne wytyczne i dobre praktyki ENISA dotyczące zarządzania ryzykiem cyberbezpieczeństwa, wdrażania wymagań NIS2 oraz bezpieczeństwa łańcucha dostaw.

W ramach usługi Wykonawca przeprowadzi co najmniej:

1. analizy dokumentacji Zamawiającego, w szczególności polityk, procedur, instrukcji, rejestrów, planów, analiz ryzyka, planów ciągłości działania, planów odtworzeniowych, dokumentacji technicznej i dokumentacji systemów teleinformatycznych oraz środowisk OT/ICS/SCADA;
2. wywiadów i warsztatów z przedstawicielami Zamawiającego, w tym z kierownictwem oraz personelem odpowiedzialnym za IT, OT, cyberbezpieczeństwo, utrzymanie ruchu, automatykę, eksploatację sieci, ochronę danych, zarządzanie kryzysowe i ciągłość działania;
3. przeglądu na miejscu (wizji) kluczowych obiektów i pomieszczeń technicznych wskazanych w pkt 2 Części wstępnej;
4. oceny dojrzałości SZBI i SZCD, obejmującej co najmniej:
   – ład organizacyjny i odpowiedzialności,
   – polityki i procedury,
   – zarządzanie ryzykiem,
   – zarządzanie incydentami,
   – zarządzanie podatnościami,
   – bezpieczeństwo zasobów informacyjnych,
   – bezpieczeństwo infrastruktury IT i OT,
   – bezpieczeństwo sieci i segmentację,
   – kontrolę dostępu,
   – zarządzanie kopiami zapasowymi i odtwarzaniem,
   – rejestrowanie i monitorowanie zdarzeń,
   – bezpieczeństwo dostawców i łańcucha dostaw,
   – zarządzanie zmianą,
   – odporność operacyjną,
   – plany ciągłości działania i odtwarzania po awarii,
   – testowanie rozwiązań awaryjnych i planów ciągłości działania,
   – świadomość i kompetencje personelu;
5. oceny zgodności z wymaganiami KRI, w szczególności w zakresie organizacji bezpieczeństwa informacji, zarządzania ryzykiem, środków technicznych i organizacyjnych, monitorowania, rozliczalności, kopii zapasowych, ciągłości działania i nadzoru nad systemami teleinformatycznymi;
6. oceny zgodności z wymaganiami uKSC, w tym w zakresie systemu zarządzania bezpieczeństwem, zarządzania incydentami, środków bezpieczeństwa, nadzoru,

dokumentowania działań oraz obowiązków podmiotów objętych regulacją, z uwzględnieniem statusu Zamawiającego na gruncie uKSC;

7. oceny zgodności i dojrzałości względem wymagań NIS2, w szczególności w obszarze:
   – polityk analizy ryzyka i bezpieczeństwa systemów informacyjnych,
   – obsługi incydentów,
   – ciągłości działania, kopii zapasowych i odtwarzania po awarii,
   – bezpieczeństwa łańcucha dostaw,
   – bezpieczeństwa nabywania, rozwoju i utrzymania systemów,
   – oceny skuteczności środków zarządzania ryzykiem,
   – cyberhigieny i szkoleń,
   – kryptografii i – tam gdzie zasadne – szyfrowania,
   – bezpieczeństwa zasobów ludzkich i kontroli dostępu,
   – stosowania uwierzytelniania wieloskładnikowego oraz bezpiecznej komunikacji;
8. oceny obszarów specyficznych dla przedsiębiorstwa wodociągowo-kanalizacyjnego, w szczególności:
   – bezpieczeństwa systemów sterowania przemysłowego i automatyki,
   – rozdzielenia i zabezpieczenia stref IT/OT,
   – połączeń zdalnych do infrastruktury technologicznej,
   – bezpieczeństwa telemetrii, przepompowni, stacji uzdatniania wody, oczyszczalni ścieków, przepływomierzy, czujników i urządzeń terenowych,
   – odporności na zakłócenia procesów technologicznych,
   – bezpieczeństwa dostępu serwisowego producentów i integratorów,
   – bezpieczeństwa aktualizacji, zmian konfiguracyjnych i prac serwisowych w środowiskach OT;
9. identyfikacji niezgodności, luk, ryzyk i podatności organizacyjnych i technicznych oraz obszarów wymagających pilnej interwencji;
10. opracowania raportu z audytu początkowego.

Minimalna zawartość raportu z audytu początkowego

1. opis celu, zakresu, kryteriów i metodyki audytu oraz składu zespołu audytowego;
2. opis stanu istniejącego;
3. ocenę zgodności z wymaganiami KRI, uKSC, NIS2 i wskazanymi normami;
4. ocenę dojrzałości SZBI i SZCD;
5. identyfikację luk, niezgodności, słabości i ryzyk;
6. ocenę wpływu stwierdzonych słabości na bezpieczeństwo świadczenia usług wodociągowo-kanalizacyjnych;

7. rekomendacje działań naprawczych, usprawniających i rozwojowych, z podziałem na organizacyjne i techniczne;
8. priorytetyzację działań według istotności, pilności i wpływu na ciągłość działania, z podziałem na działania krótko-, średnio- i długoterminowe;
9. wskazanie, które rekomendacje powinny zostać uwzględnione w dokumentacji SZBI i SZCD opracowywanej w Zadaniu nr 2;
10. macierz zgodności z wymaganiami prawnymi, normatywnymi i branżowymi;
11. podsumowanie dla kierownictwa umożliwiające podjęcie decyzji zarządczych.

1.B. Audyt cyberbezpieczeństwa sieci IT/OT/ICS

Przedmiotem usługi jest audyt cyberbezpieczeństwa sieci IT, OT i ICS Zamawiającego, obejmujący ocenę architektury, konfiguracji i zabezpieczeń sieci oraz urządzeń sieciowych. Audyt obejmuje infrastrukturę w stanie na dzień jego przeprowadzenia, w tym rozwiązania części technicznej projektu wdrożone do tego dnia, a w zakresie rozwiązań jeszcze niewdrożonych – ocenę ich planowanej architektury pod kątem segmentacji i bezpieczeństwa sieci. Audyt ma charakter przeglądu architektury i konfiguracji i uzupełnia testy bezpieczeństwa (pkt 1.C) – nie obejmuje prób wykorzystania podatności.

W zakresie OT czynności na miejscu obejmują centrum nadzoru (system SCADA) w siedzibie Zamawiającego oraz reprezentatywną próbę obiektów technologicznych wskazanych przez Zamawiającego – co najmniej 2 stacje uzdatniania wody, 2 ujęcia wody i 3 przepompownie. Ustalenia z próby Wykonawca odnosi do pozostałych obiektów o analogicznej konfiguracji, na podstawie dokumentacji i informacji przekazanych przez Zamawiającego. Ta sama próba obowiązuje w testach środowiska OT (pkt 1.C) oraz przy przeglądzie na miejscu w audycie początkowym i końcowym.

Minimalny zakres audytu

1. weryfikacja topologii sieci IT i OT, w tym aktualności schematów sieci i wykazu urządzeń sieciowych;
2. ocena architektury sieci, w tym podziału na strefy i kanały komunikacji (np. według PN-EN IEC 62443 lub równoważnego modelu), separacji IT/OT i stref pośrednich (DMZ);
3. przegląd konfiguracji urządzeń brzegowych i zapór sieciowych, w tym reguł filtrowania ruchu, z identyfikacją reguł nadmiarowych i zbyt szerokich;
4. przegląd konfiguracji przełączników i innych urządzeń sieciowych (VLAN, zabezpieczenia portów, zarządzanie urządzeniami, wersje oprogramowania);
5. ocena mechanizmów zdalnego dostępu, w tym VPN i dostępu serwisowego dostawców do środowiska OT;
6. ocena komunikacji telemetrycznej z obiektami (np. łącza GSM/LTE, radiowe, VPN) pod kątem poufności, integralności i dostępności;
7. ocena pokrycia sieci monitorowaniem i rejestrowaniem zdarzeń, w tym integracji z systemem SIEM;
8. ocena zgodności konfiguracji urządzeń sieciowych z dobrymi praktykami hardeningu (np. CIS Benchmarks lub równoważnymi);

9. ocena odporności sieci na awarie (redundancja łączy i urządzeń, zasilanie awaryjne urządzeń sieciowych).

Czynności w środowisku OT prowadzi się wyłącznie metodami nieinwazyjnymi (przegląd konfiguracji, pasywna analiza ruchu), w uzgodnieniu z Zamawiającym.

Raport z audytu sieci

Raport zawiera co najmniej:

1. zakres, metodykę i dane audytorów;
2. aktualny schemat logiczny sieci IT i OT z podziałem na strefy;
3. listę ustaleń z oceną ryzyka i priorytetem;
4. rekomendacje zmian w architekturze i konfiguracji;
5. podsumowanie dla kierownictwa.

1.C. Testy bezpieczeństwa (testy penetracyjne) IT i OT

Testy obejmują infrastrukturę w stanie na dzień ich przeprowadzenia, w tym rozwiązania części technicznej projektu wdrożone do tego dnia. Testy przeprowadza się nie później niż do dnia 18.12.2026 r., przed audytem końcowym, tak aby ich wyniki zostały uwzględnione w audycie końcowym.

Przez testy penetracyjne rozumie się testy mające na celu wykrycie i praktyczną weryfikację podatności, prowadzone przez certyfikowanego pentestera. Samo skanowanie pod kątem znanych podatności narzędziami automatycznymi (np. Nessus, OpenVAS/Greenbone, Burp Suite, Acunetix) nie spełnia wymagania testów penetracyjnych.

Zasady prowadzenia testów (rules of engagement)

1. Przed rozpoczęciem testów Wykonawca przedstawia do akceptacji Zamawiającego plan testów: zakres (adresy, systemy, wyłączenia), harmonogram i okna czasowe, metody, osoby testujące oraz kanał kontaktu awaryjnego.
2. Testy rozpoczynają się po pisemnej autoryzacji Zamawiającego. Testy mogące wpłynąć na dostępność systemów prowadzi się w uzgodnionych oknach serwisowych.
3. Wykonawca niezwłocznie przerywa testy i informuje Zamawiającego w razie zakłócenia pracy systemu lub wykrycia podatności krytycznej.
4. Testy prowadzi się zgodnie z uznaną metodyką (np. PTES, OWASP Testing Guide, NIST SP 800-115 lub równoważną).

Minimalny zakres testów

1. zewnętrzne testy penetracyjne infrastruktury (do 2 publicznych adresów IP):
   – analiza topologii i zabezpieczeń brzegu sieci;
   – weryfikacja mechanizmów ochronnych na granicy sieci, w tym zapór, systemów IDS/IPS i innych zabezpieczeń;

– identyfikacja usług udostępnionych do Internetu (skanowanie portów i usług) oraz ich wersji;

– próby wykorzystania zidentyfikowanych podatności w celu oceny ryzyka;

– rekomendacje wzmocnienia zabezpieczeń styku sieci lokalnej z Internetem;

2. wewnętrzne testy penetracyjne infrastruktury IT (do 21 adresów IP, w tym 7 stacji roboczych i 1 serwer):

– analiza topologii i zabezpieczeń sieci LAN, w tym segmentacji i izolacji urządzeń;

– skanowanie portów TCP/UDP, usług i aktywnych hostów;

– próby wykorzystania podatności w sieci LAN, w tym eskalacji uprawnień i ruchu bocznego;

– weryfikacja skuteczności systemów monitorowania i wykrywania (czy działania testowe zostały wykryte przez rozwiązania działające w dniu testów, w szczególności SIEM, SOAR i XDR – jeżeli zostały już wdrożone);

– ocena procesu tworzenia i odtwarzania kopii zapasowych;

– rekomendacje poprawy zabezpieczeń sieci LAN;

3. testy środowiska OT – **wyłącznie metodami nieinwazyjnymi**, w uzgodnieniu z Zamawiającym, w zakresie próby obiektów określonej w pkt 1.B:

– weryfikacja separacji i filtrowania ruchu między strefami IT i OT (testy prowadzone ze strefy IT i stref pośrednich);

– pasywna analiza ruchu i inwentaryzacja urządzeń OT, w tym identyfikacja niezabezpieczonych protokołów;

– przegląd konfiguracji zdalnego dostępu do systemów OT, w tym dostępu serwisowego;

– zakaz aktywnego skanowania i prób wykorzystania podatności na urządzeniach sterujących procesem technologicznym bez odrębnej, pisemnej zgody Zamawiającego;

4. audyt serwisów WWW (2 serwisy: gsk.ilawa.pl i ebok.gsk.ilawa.pl):

– wersje serwera HTTP i systemu CMS, ze wskazaniem znanych podatności;

– bezpieczeństwo komunikacji – certyfikaty X.509, wersje protokołu TLS i algorytmy kryptograficzne;

5. audyt serwisów pocztowych (1 domena: gmina-ilawa.pl) – z zastrzeżeniem pkt 2 Części wstępnej (zgoda właściciela domeny):

– poprawność wdrożenia mechanizmów SPF, DKIM i DMARC;

– bezpieczeństwo mechanizmów TLS w komunikacji pocztowej.

Raport z testów

Raport z testów zawiera co najmniej:

1. podsumowanie dla kierownictwa;

2. zakres, metodykę, harmonogram i dane osób testujących;

3. listę zidentyfikowanych podatności z oceną ryzyka (np. według CVSS), opisem sposobu wykrycia i dowodem (zrzuty ekranu, logi), z zachowaniem poufności danych dostępowych;
4. ocenę skuteczności wykrywania działań testowych przez wdrożone systemy bezpieczeństwa;
5. rekomendacje usunięcia podatności, z priorytetami;
6. informację o podatnościach krytycznych zgłoszonych Zamawiającemu w trakcie testów.

1.D. Szkolenie powiązane z testami socjotechnicznymi

Przedmiotem usługi jest przeprowadzenie kontrolowanych testów socjotechnicznych, które weryfikują świadomość zagrożeń i reakcje personelu, w szczególności osób pełniących role w SZBI, oraz szkolenia omawiającego ich wyniki.

Zakres usługi

1. uzgodnienie z Zamawiającym scenariuszy, grup docelowych, harmonogramu i zasad testów, w tym listy osób powiadomionych o testach; testy rozpoczynają się po pisemnej akceptacji Zamawiającego;
2. kampania symulowanego phishingu obejmująca wszystkich pracowników korzystających z poczty elektronicznej – co najmniej 2 scenariusze wiadomości, z pomiarem otwarć, kliknięć, wprowadzenia danych i zgłoszeń;
3. co najmniej jeden test socjotechniczny innego rodzaju (np. próba wyłudzenia informacji telefonicznie – vishing – albo test pozostawionego nośnika), w uzgodnieniu z Zamawiającym;
4. ocena, czy osoby pełniące role w SZBI zareagowały zgodnie z procedurą zgłaszania i obsługi incydentów;
5. szkolenie dla pracowników omawiające wyniki testów – w formie stacjonarnej, w siedzibie Zamawiającego, w wymiarze co najmniej 2 godzin zegarowych, z omówieniem zaobserwowanych błędów (bez wskazywania osób) i zasad prawidłowego postępowania;
6. raport z testów i szkolenia.

Zasady prowadzenia testów

1. Testy nie mogą prowadzić do pozyskania rzeczywistych haseł ani innych danych uwierzytelniających – rejestruje się wyłącznie fakt ich wprowadzenia.
2. Wyniki przekazuje się w postaci zagregowanej; dane imienne Wykonawca przekazuje wyłącznie Zamawiającemu, w zakresie niezbędnym do działań szkoleniowych, z poszanowaniem przepisów o ochronie danych osobowych.
3. Testy z wykorzystaniem domeny lub poczty Gminy Iława wymagają zgody, o której mowa w pkt 2 Części wstępnej.

Raport

Raport zawiera co najmniej: scenariusze i przebieg testów, wyniki w ujęciu statystycznym, ocenę reakcji osób pełniących role w SZBI, rekomendacje szkoleniowe i proceduralne oraz program, materiały i listę obecności ze szkolenia.

1.E. Audyt końcowy

Przedmiotem usługi jest audyt końcowy obejmujący audyt SZBI i SZCD oraz ocenę zgodności organizacyjnej, technicznej, proceduralnej i formalnoprawnej Zamawiającego. Audyt służy ocenie stanu bezpieczeństwa po realizacji działań przewidzianych w projekcie, weryfikacji wdrożenia zaleceń z audytu początkowego, ocenie skuteczności zastosowanych środków oraz potwierdzeniu poziomu zgodności. **Audyt przeprowadza się na końcu realizacji zamówienia – po odbiorze SZBI i SZCD w Zadaniu nr 2 i po odbiorze audytu sieci i testów (1.B i 1.C). Audyt obejmuje rozwiązania części technicznej projektu wdrożone do dnia jego przeprowadzenia.**

Zakres audytu musi uwzględniać specyfikę przedsiębiorstwa wodociągowo-kanalizacyjnego, w tym środowisk IT i OT, systemów sterowania, automatyki przemysłowej, telemetrii, systemów SCADA, zdalnego monitoringu oraz infrastruktury istotnej dla ciągłości zbiorowego zaopatrzenia w wodę i odprowadzania ścieków.

Audyt przeprowadza się w oparciu o przepisy, normy i dobre praktyki wskazane w pkt 1.A. W ramach usługi Wykonawca przeprowadzi co najmniej:

1. analizy dokumentacji Zamawiającego, w tym dokumentacji SZBI i SZCD opracowanej w Zadaniu nr 2 oraz dokumentacji rozwiązań części technicznej projektu – wdrożonych do dnia audytu albo planowanych do wdrożenia, w szczególności polityk, procedur, instrukcji, rejestrów, analiz ryzyka, planów ciągłości działania i planów odtworzeniowych oraz dokumentacji środowisk OT/ICS/SCADA;
2. wywiadów i warsztatów z przedstawicielami Zamawiającego, w tym z kierownictwem oraz personelem odpowiedzialnym za IT, OT, cyberbezpieczeństwo, utrzymanie ruchu, automatykę, eksploatację sieci, ochronę danych, zarządzanie kryzysowe i ciągłość działania;
3. przeglądu na miejscu (wizji) kluczowych obiektów i pomieszczeń technicznych wskazanych w pkt 2 Części wstępnej;
4. oceny dojrzałości SZBI i SZCD, obejmującej co najmniej:
   – ład organizacyjny i odpowiedzialności,
   – polityki i procedury,
   – zarządzanie ryzykiem,
   – zarządzanie incydentami,
   – zarządzanie podatnościami,
   – bezpieczeństwo zasobów informacyjnych,
   – bezpieczeństwo infrastruktury IT i OT,
   – bezpieczeństwo sieci i segmentację,

– kontrolę dostępu,

– zarządzanie kopiami zapasowymi i odtwarzaniem,

– rejestrowanie i monitorowanie zdarzeń,

– bezpieczeństwo dostawców i łańcucha dostaw,

– zarządzanie zmianą,

– odporność operacyjną,

– plany ciągłości działania i odtwarzania po awarii,

– testowanie rozwiązań awaryjnych i planów ciągłości działania,

– świadomość i kompetencje personelu;

5. oceny zgodności z wymaganiami KRI, w szczególności w zakresie organizacji bezpieczeństwa informacji, zarządzania ryzykiem, środków technicznych i organizacyjnych, monitorowania, rozliczalności, kopii zapasowych, ciągłości działania i nadzoru nad systemami teleinformatycznymi;
6. oceny zgodności z wymaganiami uKSC, w tym w zakresie systemu zarządzania bezpieczeństwem, zarządzania incydentami, środków bezpieczeństwa, nadzoru, dokumentowania działań oraz obowiązków podmiotów objętych regulacją, z uwzględnieniem statusu Zamawiającego na gruncie uKSC;
7. oceny zgodności i dojrzałości względem wymagań NIS2, w szczególności w obszarze:

– polityk analizy ryzyka i bezpieczeństwa systemów informacyjnych,

– obsługi incydentów,

– ciągłości działania, kopii zapasowych i odtwarzania po awarii,

– bezpieczeństwa łańcucha dostaw,

– bezpieczeństwa nabywania, rozwoju i utrzymania systemów,

– oceny skuteczności środków zarządzania ryzykiem,

– cyberhigieny i szkoleń,

– kryptografii i – tam gdzie zasadne – szyfrowania,

– bezpieczeństwa zasobów ludzkich i kontroli dostępu,

– stosowania uwierzytelniania wieloskładnikowego oraz bezpiecznej komunikacji;

8. oceny obszarów specyficznych dla przedsiębiorstwa wodociągowo-kanalizacyjnego, w szczególności:

– bezpieczeństwa systemów sterowania przemysłowego i automatyki,

– rozdzielenia i zabezpieczenia stref IT/OT,

– połączeń zdalnych do infrastruktury technologicznej,

– bezpieczeństwa telemetrii, przepompowni, stacji uzdatniania wody, oczyszczalni ścieków, przepływomierzy, czujników i urządzeń terenowych,

– odporności na zakłócenia procesów technologicznych,

– bezpieczeństwa dostępu serwisowego producentów i integratorów,

– bezpieczeństwa aktualizacji, zmian konfiguracyjnych i prac serwisowych w środowiskach OT;

9. weryfikacji stopnia realizacji zaleceń z audytu początkowego oraz oceny skuteczności wdrożonych działań naprawczych, organizacyjnych i technicznych;
10. uwzględnienia wyników audytu sieci, testów bezpieczeństwa i testów socjotechnicznych przeprowadzonych w pkt 1.B–1.D;
11. oceny, czy wdrożone rozwiązania podniosły poziom bezpieczeństwa, odporności operacyjnej i ciągłości działania Zamawiającego;
12. identyfikacji niezgodności, luk, ryzyk resztkowych i obszarów wymagających dalszych działań doskonalących;
13. opracowania raportu z audytu końcowego.

Minimalna zawartość raportu z audytu końcowego

1. opis celu, zakresu, kryteriów i metodyki audytu oraz składu zespołu audytowego;
2. opis stanu na dzień zakończenia audytu;
3. ocenę zgodności z wymaganiami KRI, uKSC, NIS2 i wskazanymi normami;
4. ocenę dojrzałości SZBI i SZCD, w porównaniu z wynikami audytu początkowego;
5. ocenę stopnia wdrożenia zaleceń z audytu początkowego (tabela: zalecenie – stan – ocena);
6. odniesienie do wyników audytu sieci, testów bezpieczeństwa i testów socjotechnicznych;
7. identyfikację pozostających luk, niezgodności i ryzyk resztkowych;
8. ocenę wpływu wdrożonych rozwiązań na bezpieczeństwo świadczenia usług wodociągowo-kanalizacyjnych;
9. macierz zgodności z wymaganiami prawnymi, normatywnymi i branżowymi;
10. rekomendacje dalszego doskonalenia;
11. podsumowanie dla kierownictwa, umożliwiające ocenę osiągniętego poziomu zgodności i potwierdzające efekty projektu na potrzeby jego rozliczenia.

1.F. Wymagania wobec sposobu realizacji Zadania nr 1

1. Wykonawca przeprowadza audyty i testy w sposób niezależny, obiektywny i bezstronny. Osoby realizujące Zadanie nr 1 nie mogą uczestniczyć w realizacji Zadania nr 2 ani odpowiadać za wdrożenie, przegląd lub utrzymanie audytowanych systemów.
2. Wnioski muszą uwzględniać zarówno ogólne wymagania systemowe, jak i specyfikę branży wodociągowo-kanalizacyjnej, w tym ciągłość usług publicznych, bezpieczeństwo procesów technologicznych i niezawodność infrastruktury.
3. Audyty prowadzi się w formie stacjonarnej, w siedzibie Zamawiającego i obiektach wskazanych w pkt 2 Części wstępnej, w wymiarze co najmniej 2 dni roboczych na

miejscu dla audytu początkowego i co najmniej 1 dnia roboczego na miejscu dla audytu końcowego. Forma zdalna jest dopuszczalna wyłącznie dla czynności uzupełniających. Testy zewnętrzne mogą być prowadzone zdalnie.

4. Raporty podpisują: z audytu początkowego i końcowego – audytor SZBI i audytor cyberbezpieczeństwa wskazani w ofercie; z audytu sieci – audytor cyberbezpieczeństwa; z testów bezpieczeństwa i testów socjotechnicznych – pentester wskazany w ofercie.
5. Wykonawca przedstawi wyniki każdego audytu i testów kierownictwu Zamawiającego na spotkaniu podsumowującym.

ZADANIE NR 2 – OPRACOWANIE I WDROŻENIE SZBI I SZCD WRAZ ZE SZKOLENIAMI

2.A–2.B. Opracowanie i wdrożenie SZBI (2.A) oraz SZCD (2.B)

Przedmiotem usługi jest opracowanie, dostosowanie i wdrożenie kompletnej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji („SZBI") oraz Systemu Zarządzania Ciągłością Działania w obszarze systemów teleinformatycznych („SZCD"), na podstawie wyników audytu początkowego, z uwzględnieniem stanu organizacyjnego, technicznego i formalnoprawnego Zamawiającego.

Pozycja 2.A obejmuje dokumenty minimalne nr 1–5 i 7 oraz wdrożenie SZBI. Pozycja 2.B obejmuje dokument minimalny nr 6 (dokumentacja SZCD) oraz wdrożenie SZCD. Pozycje podlegają odrębnym odbiorom; dopuszcza się ich odbiór w tym samym terminie.

Zamawiający przekaże Wykonawcy raport z audytu początkowego (Zadanie nr 1) niezwłocznie po jego odbiorze. Wykonawca uwzględnia wyniki i rekomendacje raportu, a w wykazie dokumentów wskazuje, które rekomendacje zostały zaadresowane w poszczególnych dokumentach.

Wykonawca rozpoczyna prace od dnia zawarcia umowy, na podstawie własnej analizy stanu wyjściowego (analizy luk), wykonanej w ramach wynagrodzenia za pozycje 2.A i 2.B. Po otrzymaniu raportu z audytu początkowego Wykonawca uwzględnia jego rekomendacje przed odbiorem dokumentacji (szczegóły – § 2 ust. 4 Wzoru umowy dla Zadania nr 2).

Dokumentacja musi być spójna, kompletna, praktyczna i dostosowana do specyfiki przedsiębiorstwa wodociągowo-kanalizacyjnego, jego struktury, procesów, infrastruktury, środowisk IT i OT, automatyki, telemetrii, SCADA i zdalnego monitoringu. Musi umożliwiać faktyczne stosowanie, a nie mieć wyłącznie charakter formalny.

Dokumentację opracowuje się w oparciu o przepisy, normy i dobre praktyki wskazane w pkt 1.A oraz rozporządzenie (UE) 2016/679 (RODO) i ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych.

Zakres merytoryczny dokumentacji

1. zasady organizacji bezpieczeństwa informacji i cyberbezpieczeństwa;
2. zasady zarządzania ryzykiem w obszarze informacji, systemów teleinformatycznych, cyberbezpieczeństwa i ciągłości działania;

3. zasady klasyfikacji informacji, ochrony zasobów i odpowiedzialności za zasoby;
4. zasady ochrony systemów teleinformatycznych, sieci, stanowisk roboczych, serwerów, urządzeń mobilnych oraz środowisk IT i OT;
5. zasady ochrony systemów automatyki, telemetrii, zdalnych połączeń technicznych i SCADA;
6. zasady zarządzania incydentami, w tym obsługi incydentów i ich zgłaszania zgodnie z uKSC, oraz naruszeniami ochrony danych osobowych;
7. zasady zapewnienia ciągłości działania systemów teleinformatycznych i procesów krytycznych;
8. zasady tworzenia, testowania, przechowywania i odtwarzania kopii zapasowych;
9. zasady nadzoru nad dostawcami i bezpieczeństwem łańcucha dostaw;
10. zasady monitorowania, przeglądów, testów, audytów wewnętrznych, działań korygujących i doskonalenia;
11. zasady zgodności z wymaganiami KRI, uKSC, RODO i NIS2.

Wymagania wobec dokumentacji

– dostosowanie do rzeczywistych warunków organizacyjnych i technicznych Zamawiającego, w tym do rozwiązań wdrożonych lub planowanych do wdrożenia w części technicznej projektu;

– oparcie na wynikach audytu początkowego i zidentyfikowanych ryzykach;

– wzory rejestrów, formularzy, upoważnień, ewidencji, raportów, planów i oświadczeń – tam, gdzie są niezbędne do stosowania dokumentacji;

– forma umożliwiająca przyjęcie dokumentów aktami wewnętrznymi Zamawiającego (wraz z projektami tych aktów);

– spójność dokumentów głównych, procedur i załączników oraz powiązanie SZBI, SZCD, ochrony danych, zarządzania incydentami i ryzykiem;

– podział odpowiedzialności między kierownictwo, administratorów, użytkowników i osoby odpowiedzialne za infrastrukturę technologiczną i cyberbezpieczeństwo.

Dokumenty minimalne

1. Polityka Bezpieczeństwa Informacji, w szczególności:
   – cele bezpieczeństwa informacji i zasady ich monitorowania;
   – kontekst organizacji, strony zainteresowane, czynniki wewnętrzne i zewnętrzne;
   – zakres SZBI;
   – zasady zarządzania dokumentacją systemową;
   – role, odpowiedzialności i uprawnienia;
   – nadzór kierownictwa, przeglądy zarządzania i doskonalenie;
   – klasyfikacja informacji i postępowanie z informacjami;
   – zasady czystego biurka i czystego ekranu;

– bezpieczeństwo zasobów ludzkich i dopuszczanie użytkowników do pracy;

– zgłaszanie i obsługa incydentów;

– monitorowanie zgodności z wymaganiami.

2. Polityka Bezpieczeństwa Teleinformatycznego, w szczególności procedury:

– zarządzania dostępem i uprawnieniami;

– uwierzytelniania, haseł i uwierzytelniania wieloskładnikowego;

– bezpieczeństwa sieci oraz segmentacji i separacji środowisk IT i OT;

– korzystania z poczty elektronicznej i Internetu, pracy zdalnej, urządzeń mobilnych i nośników;

– szyfrowania i stosowania kryptografii;

– kopii zapasowych (wykonywanie, przechowywanie, testowanie, odtwarzanie);

– monitorowania, rejestrowania zdarzeń i przeglądu logów;

– zarządzania podatnościami, aktualizacjami i zmianą;

– przeglądów i konserwacji systemów oraz bezpiecznej utylizacji nośników;

– ewidencja sprzętu, oprogramowania i kont uprzywilejowanych, rejestr połączeń zdalnych (VPN), wzory raportów administratora.

3. Polityka Bezpieczeństwa Fizycznego i Środowiskowego, w szczególności:

– ochrona fizyczna budynków, pomieszczeń i stref, w tym obiektów technologicznych;

– zarządzanie kluczami, kartami i kodami dostępu;

– wykaz obszarów przetwarzania informacji i obszarów wrażliwych (serwerownie, sterownie, pomieszczenia techniczne);

– ewidencja osób upoważnionych i nadzór nad gośćmi, serwisantami i podmiotami zewnętrznymi;

– reagowanie na zdarzenia fizyczne.

4. Polityka Ochrony Danych Osobowych, w szczególności:

– zasady przetwarzania danych i realizacji obowiązków administratora;

– upoważnienia do przetwarzania danych i ich ewidencja, oświadczenia o poufności;

– wzory umów powierzenia i ich wykaz, wzory dokumentów realizacji praw osób, rejestr żądań;

– wzór rejestru czynności przetwarzania (i – jeżeli zasadne – rejestru kategorii czynności);

– metodyka szacowania ryzyka dla ochrony danych, zintegrowana z ryzykiem bezpieczeństwa informacji;

– procedura postępowania z naruszeniami ochrony danych wraz ze wzorami dokumentów.

5. Dokumentacja zarządzania ryzykiem:

– metodyka szacowania ryzyka dla bezpieczeństwa informacji, cyberbezpieczeństwa, ciągłości działania i ochrony danych osobowych;

– kryteria oceny prawdopodobieństwa, skutku, poziomu i akceptacji ryzyka;

– zasady postępowania z ryzykiem;

– wzory karty ryzyka, rejestru ryzyk i planu postępowania z ryzykiem;

– **pierwsza analiza ryzyka przeprowadzona wspólnie z Zamawiającym według opracowanej metodyki**;

– powiązanie wyników analizy ryzyka z doborem zabezpieczeń.

6. Dokumentacja SZCD dla systemów teleinformatycznych:

– polityka i zakres SZCD;

– identyfikacja procesów krytycznych i zasobów wspierających;

– **analiza wpływu na działalność (BIA) przeprowadzona dla obszaru teleinformatycznego Zamawiającego**;

– analiza zagrożeń i scenariuszy zakłócających;

– zasady opracowywania i utrzymywania planów ciągłości działania i odtwarzania po awarii (same plany – pkt 2.C);

– organizacja pracy awaryjnej, komunikacja kryzysowa i eskalacja;

– zasady testowania planów i dokumentowania testów oraz przeglądu SZCD.

7. Dokumentacja dla środowisk IT/OT/SCADA – procedury lub zasady dotyczące:

– zarządzania dostępem do systemów OT/SCADA;

– rozdziału stref i połączeń IT–OT;

– dostępu serwisowego dostawców i integratorów;

– aktualizacji, zmian konfiguracji i prac utrzymaniowych w środowisku technologicznym;

– postępowania w razie awarii lub incydentu w infrastrukturze technologicznej;

– dokumentowania zmian w środowisku OT;

– ograniczania ryzyka dla procesów dostaw wody i odbioru ścieków.

Wdrożenie

1. Wykonawca przedstawia projekt dokumentacji do zatwierdzenia przez Zamawiającego. Zamawiający zgłasza uwagi na zasadach określonych w pkt 6 Części wstępnej.
2. Po zatwierdzeniu Wykonawca wdraża SZBI i SZCD w zakresie organizacyjnym i proceduralnym, w szczególności: przygotowuje projekty aktów wewnętrznych wprowadzających dokumentację, przeprowadza warsztaty wdrożeniowe z osobami pełniącymi role w SZBI i SZCD (co najmniej 1 dzień roboczy na miejscu), wspiera Zamawiającego w uzupełnieniu rejestrów i ewidencji oraz w przeprowadzeniu pierwszej analizy ryzyka i BIA.

3. Wdrożenie nie obejmuje zmian konfiguracji systemów technicznych.

Rezultaty

1. kompletna dokumentacja SZBI i SZCD wraz z załącznikami, rejestrami, wzorami i ewidencjami;
2. projekty aktów wewnętrznych wprowadzających dokumentację;
3. wyniki pierwszej analizy ryzyka i BIA;
4. mapa dokumentów z określeniem ich powiązań oraz wskazaniem zaadresowanych rekomendacji audytu początkowego;
5. wykaz wymagań prawnych, normatywnych i organizacyjnych, do których odnosi się dokumentacja;
6. wersja edytowalna dokumentacji.

2.C. Plany ciągłości działania (BCP) i plany odtwarzania po awarii (DRP) dla systemów teleinformatycznych

Przedmiotem usługi jest opracowanie planów ciągłości działania (BCP) i planów odtwarzania po awarii (DRP) dla systemów teleinformatycznych Zamawiającego, w tym systemów IT i OT wspierających zaopatrzenie w wodę i odprowadzanie ścieków. Plany muszą być spójne z dokumentacją SZCD (pkt 2.B) oraz z wynikami analizy wpływu na działalność (BIA) i analizy ryzyka.

Minimalna zawartość planów

1. wykaz systemów i usług krytycznych objętych planami, z przypisaniem właścicieli i parametrów RTO, RPO i MTPD;
2. scenariusze zakłóceń, co najmniej: atak ransomware, utrata serwera lub serwerowni, awaria łączy i sieci, utrata systemu SCADA lub telemetrii, awaria zasilania, niedostępność kluczowego dostawcy lub personelu;
3. dla każdego scenariusza – kryteria uruchomienia planu, skład i zadania zespołu, procedury awaryjne (w tym ręczne prowadzenie procesów technologicznych), komunikację wewnętrzną i zewnętrzną oraz kryteria powrotu do normalnej pracy;
4. procedury odtworzeniowe (DRP) dla systemów krytycznych – krok po kroku, z kolejnością odtwarzania i zależnościami, z wykorzystaniem kopii zapasowych i rozwiązań wdrożonych lub planowanych do wdrożenia w części technicznej projektu (serwer, macierz dyskowa, usługi wysokiej dostępności);
5. listy kontaktowe i wzory komunikatów (do uzupełnienia danymi przez Zamawiającego);
6. plan testów BCP i DRP na 12 miesięcy po zakończeniu projektu oraz wzór raportu z testu.

Plany mają mieć formę praktyczną – zwięzłe karty postępowania dla osób wykonujących, a nie wyłącznie opisy ogólne. Plany przedstawia się do zatwierdzenia na zasadach pkt 6 Części wstępnej.

2.D. Utrzymanie i doskonalenie SZBI

Przedmiotem usługi jest wsparcie Zamawiającego w utrzymaniu i doskonaleniu SZBI w okresie od dnia zatwierdzenia dokumentacji SZBI do dnia 22.12.2026 r., tak aby system funkcjonował w praktyce.

Zakres usługi

1. przeprowadzenie, wspólnie z Zamawiającym, pierwszego przeglądu zarządzania SZBI zgodnie z pkt 9.3 PN-EN ISO/IEC 27001, z przygotowaniem danych wejściowych i protokołu;
2. opracowanie planu działań SZBI na 12 miesięcy po zakończeniu projektu (przeglądy, audyty wewnętrzne, testy, szkolenia, aktualizacje dokumentacji);
3. uzupełnienie rejestrów SZBI (aktywów, ryzyk, incydentów, uprawnień) o dane dotyczące rozwiązań wdrożonych lub planowanych do wdrożenia w części technicznej projektu;
4. aktualizacja planu postępowania z ryzykiem o ustalenia przekazane przez Zamawiającego w okresie świadczenia usługi, w szczególności wyniki audytu sieci i testów bezpieczeństwa;
5. konsultacje dla osób pełniących role w SZBI – zdalnie, w wymiarze do 8 godzin;
6. sprawozdanie z utrzymania SZBI, obejmujące wykonane czynności i stan realizacji planu działań.

2.E. Doradztwo w zakresie warunków umów z dostawcami

Przedmiotem usługi jest doradztwo w zakresie warunków umów na wdrożenie i utrzymanie infrastruktury w zakresie cyberbezpieczeństwa IT/OT/ICS, obejmujących w szczególności bezpieczeństwo łańcucha dostaw, infrastrukturę monitorowania i zarządzania oraz usługi zdalne.

Zakres usługi

1. przegląd obowiązujących umów Zamawiającego z dostawcami i usługodawcami, którzy mają dostęp do systemów IT lub OT albo świadczą usługi ICT (2 umowy), pod kątem wymagań bezpieczeństwa;
2. katalog wymagań bezpieczeństwa (klauzul umownych) do stosowania w umowach z dostawcami ICT, obejmujący co najmniej: dostęp zdalny i serwisowy, poufność i ochronę danych, zgłaszanie incydentów i podatności wraz z terminami, aktualizacje i wsparcie bezpieczeństwa w cyklu życia produktu, podwykonawstwo i łańcuch dostaw, prawo do audytu, ciągłość świadczenia usług i parametry SLA, zakończenie współpracy i zwrot danych, zgodność z uKSC;
3. wzór aneksu wprowadzającego wymagania bezpieczeństwa do zawartych umów;
4. lista kontrolna oceny dostawcy przed zawarciem umowy;
5. rekomendacje dotyczące poszczególnych umów objętych przeglądem;
6. konsultacja z osobami odpowiedzialnymi za zawieranie umów, w wymiarze co najmniej 2 godzin.

2.F. Podstawowe szkolenie z zakresu cyberbezpieczeństwa dla pracowników

Wykonawca przeprowadzi szkolenie dla 10 **uczestników, w 1 grupie, w wymiarze co najmniej 4 godzin zegarowych, w formie stacjonarnej**, w siedzibie Zamawiającego. Szkolenie składa się z dwóch segmentów.

Segment I – ogólny

1. cyberbezpieczeństwo w przedsiębiorstwie wodociągowo-kanalizacyjnym – znaczenie dla informacji, systemów IT i OT/ICS/SCADA i ciągłości usług;
2. rola pracowników IT i OT w zapewnieniu bezpieczeństwa;
3. podstawowe zasady ochrony danych, kont, zasobów, systemów sterowania i urządzeń terenowych;
4. zagrożenia dla środowisk IT i OT (phishing, socjotechnika, ransomware, malware, nieautoryzowany dostęp, błędy konfiguracji, niekontrolowane połączenia zdalne);
5. phishing i inne ataki socjotechniczne – rozpoznawanie i reagowanie;
6. bezpieczna poczta elektroniczna i komunikacja służbowa;
7. hasła, uwierzytelnianie wieloskładnikowe, ochrona kont uprzywilejowanych;
8. zarządzanie dostępem i zasada minimalnych uprawnień;
9. bezpieczny dostęp zdalny i serwisowy;
10. segmentacja IT/OT – znaczenie i zasady;
11. bezpieczeństwo stacji roboczych, stacji operatorskich, telemetrii i urządzeń terenowych;
12. aktualizacje i zarządzanie konfiguracją, ze specyfiką OT;
13. bezpieczeństwo prac serwisowych i współpracy z wykonawcami zewnętrznymi;
14. kopie zapasowe i odtwarzanie;
15. reagowanie na incydenty w IT i OT;
16. ciągłość działania przedsiębiorstwa;
17. dobre praktyki i najczęstsze błędy.

Segment II – rozwiązania wdrożone u Zamawiającego

Segment przygotowuje pracowników do codziennej pracy z uwzględnieniem wdrożonych SZBI i SZCD oraz rozwiązań części technicznej projektu – wdrożonych do dnia szkolenia albo planowanych do wdrożenia. Wykonawca, przed szkoleniem, zapoznaje się z rozwiązaniami uruchomionymi lub planowanymi przez Zamawiającego oraz z przyjętymi procedurami, a następnie opracowuje program i materiały. Katalog tematów ma charakter ramowy – Wykonawca uwzględnia je w zakresie, w jakim znajdują zastosowanie:

1. zmiany w zasadach logowania i uwierzytelniania (MFA, klucze sprzętowe, polityka haseł);
2. praca ze stacjami chronionymi przez XDR i ochronę przed ransomware – czego system pilnuje i jakich działań unikać;

3. korzystanie z sieci objętej kontrolą dostępu i segmentacją – podłączanie urządzeń, zakaz urządzeń prywatnych, VPN;
4. postępowanie z danymi i kopiami zapasowymi;
5. monitorowanie i rejestrowanie zdarzeń (SIEM) – znaczenie dla odpowiedzialności i higieny pracy;
6. zgłaszanie incydentów według procedur SZBI;
7. postępowanie w sytuacjach awaryjnych według planów SZCD;
8. zasady pracy w środowisku OT dla pracowników mających styczność z systemami sterowania.

Treści przedstawia się w sposób dostosowany do kadry nietechnicznej, na przykładach z realnych procesów Zamawiającego.

2.G. Szkolenie specjalistyczne dla kadry zarządzającej i pracowników IT

Szkolenie składa się z dwóch modułów, prowadzonych odrębnie dla każdej grupy. Dotyczy środków bezpieczeństwa zastosowanych lub planowanych do zastosowania w projekcie oraz wdrożonych SZBI i SZCD.

Moduł I – kadra zarządzająca

Wykonawca przeprowadzi szkolenie z wdrożonych SZBI i SZCD dla kadry zarządzającej oraz osób odpowiedzialnych za bezpieczeństwo informacji, cyberbezpieczeństwo, ciągłość działania, IT i OT/ICS oraz pełniących funkcje decyzyjne i nadzorcze – dla 2 **uczestników, w 1 grupie, w wymiarze co najmniej 4 godzin zegarowych, w formie stacjonarnej**.

Minimalny zakres szkolenia:

1. rola SZBI i SZCD w przedsiębiorstwie wodociągowo-kanalizacyjnym;
2. podstawy prawne i normatywne: KRI, uKSC (w tym obowiązki i odpowiedzialność kierownictwa), RODO, NIS2, normy ISO 27001, 27002, 27005, 22301;
3. struktura dokumentacji SZBI (PBI, PBT, PBF, procedury) i zasady jej stosowania;
4. SZCD – procesy krytyczne, plany ciągłości działania, procedury awaryjne, rola kadry;
5. zarządzanie ryzykiem, w tym rola kierownictwa w akceptacji ryzyka;
6. role i odpowiedzialności w SZBI i SZCD;
7. zarządzanie incydentami i naruszeniami;
8. bezpieczeństwo środowisk IT/OT/ICS w ujęciu zarządczym;
9. nadzór nad dokumentacją, przeglądy, audyty i doskonalenie;
10. budowanie kultury bezpieczeństwa.

Szkolenie musi być powiązane z opracowaną dokumentacją, mieć charakter praktyczny (przykłady sytuacji decyzyjnych i incydentów, dyskusja, omówienie przypadków) i wspierać stosowanie dokumentacji.

Moduł II – pracownicy IT

Wykonawca przeprowadzi szkolenie dla 1 **osoby z kadry IT, w wymiarze co najmniej 8 godzin, w formie stacjonarnej**, przygotowujące do obsługi, konfiguracji, monitorowania i utrzymania rozwiązań części technicznej projektu – wdrożonych do dnia szkolenia albo planowanych do wdrożenia – oraz infrastruktury Zamawiającego, zgodnie z SZBI i SZCD. W zakresie rozwiązań jeszcze niewdrożonych szkolenie obejmuje zasady ich działania, konfiguracji i eksploatacji, na podstawie informacji przekazanych przez Zamawiającego. Zakres ramowy:

1. obsługa systemu SIEM – źródła danych, reguły korelacji, raporty, analiza zdarzeń;
2. obsługa systemu SOAR – scenariusze automatycznej reakcji (playbooki), obsługa zgłoszeń;
3. administrowanie XDR i ochroną przed ransomware – polityki, reagowanie na wykrycia, analiza incydentów;
4. zarządzanie podatnościami – skanowanie, priorytetyzacja, weryfikacja usunięcia; symulacje ataków (BAS);
5. monitorowanie infrastruktury informatycznej;
6. warstwa serwerowa, macierz dyskowa, usługi wysokiej dostępności i kopie zapasowe – praktyczne odtwarzanie;
7. zarządzanie tożsamością i dostępem, w tym w środowisku OT; konta uprzywilejowane i MFA;
8. współpraca z usługą SOC/MDR i wykorzystanie informacji o zagrożeniach (CTI);
9. segmentacja sieci i separacja środowiska OT;
10. dobre praktyki administrowania i dokumentowania zmian;
11. reagowanie na incydenty z poziomu wdrożonych narzędzi, w powiązaniu z SZBI i SZCD.

Co najmniej 50% czasu szkolenia stanowią zajęcia praktyczne na środowisku Zamawiającego lub środowisku je odwzorowującym, prowadzone w sposób niezakłócający pracy systemów produkcyjnych.

2.H. Szkolenie symulacyjne z zakresu cyberbezpieczeństwa, ciągłości działania i zarządzania kryzysowego

Wykonawca przeprowadzi szkolenie symulacyjne (ćwiczenie) dla kadry zarządzającej, osób pełniących role w SZBI i SZCD oraz pracowników IT i OT – dla 5 uczestników, w 1 grupie, w wymiarze co najmniej 4 godzin zegarowych, w formie stacjonarnej w siedzibie Zamawiającego.

Wymagania

1. ćwiczenie ma formę gry decyzyjnej (table-top) prowadzonej przez moderatora, z co najmniej 2 scenariuszami realistycznymi dla przedsiębiorstwa wodociągowo-kanalizacyjnego, np. atak ransomware na systemy IT z ryzykiem przeniesienia do OT oraz utrata łączności z obiektami telemetrycznymi lub systemem SCADA;

2. scenariusze opracowuje się na podstawie zatwierdzonej dokumentacji SZBI, SZCD oraz planów BCP i DRP; szczegóły Wykonawca uzgadnia z Zamawiającym;
3. ćwiczenie obejmuje: rozpoznanie i klasyfikację zdarzenia, eskalację, decyzje kierownictwa, uruchomienie planów ciągłości działania i procedur awaryjnych (w tym pracy ręcznej), komunikację wewnętrzną i zewnętrzną (w tym zgłoszenie incydentu do właściwego CSIRT i komunikaty dla odbiorców wody) oraz powrót do normalnej pracy;
4. ćwiczenie nie może zakłócać pracy systemów produkcyjnych;
5. po ćwiczeniu Wykonawca przeprowadza omówienie i przekazuje raport z ćwiczenia: przebieg, ocenę działań, zidentyfikowane braki w procedurach i rekomendacje zmian w dokumentacji SZBI, SZCD oraz planach BCP i DRP.

2.I. Certyfikacja kompetencji osób

Przedmiotem usługi jest zapewnienie 2 osobom wskazanym przez Zamawiającego udziału w egzaminie certyfikacyjnym potwierdzającym kompetencje z zakresu cyberbezpieczeństwa lub bezpieczeństwa informacji.

Wymagania

1. certyfikat wydaje niezależna od Wykonawcy jednostka lub organizacja certyfikująca; certyfikat musi być uznany na rynku (np. certyfikat audytora wewnętrznego lub osoby wdrażającej system zgodny z PN-EN ISO/IEC 27001, certyfikat z zakresu cyberbezpieczeństwa uznanego programu certyfikacji lub równoważny); rodzaj certyfikatu Wykonawca uzgadnia z Zamawiającym w terminie 3 dni roboczych od zawarcia umowy, z uwzględnieniem roli tej osoby w SZBI;
2. usługa obejmuje opłatę egzaminacyjną, organizację egzaminu (stacjonarnie albo zdalnie z nadzorem) oraz – jeżeli program certyfikacji tego wymaga – przygotowanie do egzaminu;
3. egzamin musi się odbyć nie później niż do dnia 22.12.2026 r.;
4. podstawą odbioru jest dokument potwierdzający przystąpienie do egzaminu oraz – jeżeli wynik jest dostępny – certyfikat lub zaświadczenie o wyniku; wynagrodzenie nie zależy od wyniku egzaminu.

2.J. Wymagania wobec sposobu realizacji Zadania nr 2

1. Opracowanie dokumentacji, doradztwo (2.E) i konsultacje w ramach utrzymania SZBI (2.D) mogą odbywać się zdalnie. Warsztaty wdrożeniowe (2.A i 2.B), przegląd zarządzania (2.D) i wszystkie szkolenia (2.F, 2.G, 2.H) odbywają się stacjonarnie w siedzibie Zamawiającego.
2. Terminy szkoleń Wykonawca uzgadnia z Zamawiającym z co najmniej 3-dniowym (dni robocze) wyprzedzeniem, z uwzględnieniem organizacji pracy zmianowej i ciągłości usług.
3. Szkolenia prowadzą osoby wskazane w ofercie. Wykonawca zapewnia materiały szkoleniowe dla każdego uczestnika (w wersji elektronicznej, a na życzenie –

papierowej), listy obecności, ankiety ewaluacyjne oraz imienne certyfikaty lub zaświadczenia ukończenia szkolenia.

4. Po każdym szkoleniu Wykonawca przekazuje Zamawiającemu: program, materiały, listy obecności, kopie certyfikatów i zestawienie wyników ankiet – jako podstawę odbioru i rozliczenia projektu.
5. Segment II szkolenia 2.F, Moduł II szkolenia 2.G oraz szkolenie symulacyjne 2.H odbywają się po zatwierdzeniu dokumentacji SZBI i SZCD. Dotyczą rozwiązań części technicznej projektu wdrożonych do dnia szkolenia oraz rozwiązań planowanych do wdrożenia, na podstawie informacji przekazanych przez Zamawiającego.