Zamawiający: Gmina Lubartów

ul. Lubelska 18A, 21-100 Lubartów, NIP: 7141996904 REGON: 431019951 tel.: 81 855 35 86, email: ug@gmina-lubartow.pl

Numer sprawy: ZP.271.7.2027.RF

ZAŁĄCZNIK 1A DO SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA DLA CZĘŚCI 1

dla zamówienia o wartości nieprzekraczającej 216 000,00 euro, co stanowi równowartość kwoty 930 960,00 złotych pod nazwą

„ZWIĘKSZENIE POZIOMU CYBERBEZPIECZEŃSTWA WODOCIĄGÓW W GMINIE LUBARTÓW”

Zamówienie realizowane jest w ramach projektu grantowego pod nazwą „Cyberbezpieczne Wodociągi” – Krajowy Plan Odbudowy i Zwiększania Odporności finansowany ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności, Inwestycja C3.1.1. Cyberbezpieczńsowto – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo Cyberbezpieczeństwo – Cyberbezpieczne Wodociągi.

Podpisane elektronicznie przez Marek Adam Woźniak (Certyfikat kwalifikowany) w dniu 2026-11-09.

Zamawiający określa, że przedmiotem niniejszego postępowania w części 1 o udzielenie zamówienia jest realizacja usług związanych z opracowaniem dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji, realizacja usług szkoleniowych z zakresu Systemu Zarządzania Bezpieczeństwem Informacji oraz realizacja usług audytorskich. . Zamówienie realizowane jest zgodnie założeniami projektu grantowego pod nazwą „Cyberbezpieczne Wodociągi" – Krajowy Plan Odbudowy i Zwiększania Odporności finansowany ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności, Inwestycja C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo Cyberbezpieczeństwo – Cyberbezpieczne Wodociągi.

Niniejszy dokument obejmuje wymagania dotyczące przedmiotu zamówienia.

Zakres dokumentu

Rozdział	Przedmiot zamówienia
1	Opracowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji
2	Szkolenie z zakresu cyberbezpieczeństwa dla kadry kierowniczej z zakresu wdrażanego Systemu Zarządzania Bezpieczeństwem Informacji
3	Audyt końcowy obejmujący zgodność z KRI, uoKSC oraz SZBI

1. Opracowanie i wdrożenie system Zarządzania Bezpieczeństwem Informacji

Przedmiotem zamówienia jest realizacja usługi polegającej na opracowaniu, dostosowaniu oraz przygotowaniu do wdrożenia kompletnej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji, zwanego dalej „SZBI" z uwzględnieniem stanu organizacyjnego, technicznego i formalnoprawnego Zamawiającego.

Celem usługi jest opracowanie spójnej, kompletnej i praktycznej dokumentacji systemowej, dostosowanej do specyfiki przedsiębiorstwa wodociągowo-kanalizacyjnego, jego struktury organizacyjnej, realizowanych procesów, wykorzystywanej infrastruktury, posiadanych zasobów informacyjnych, środowisk IT i OT, systemów automatyki przemysłowej, telemetryki, systemów SCADA, zdalnego monitoringu oraz wymagań związanych z zapewnieniem ciągłości świadczenia usług zbiorowego zaopatrzenia w wodę i odprowadzania ścieków.

Dokumentacja musi zostać opracowana w sposób umożliwiający jej faktyczne wdrożenie i stosowanie przez Zamawiającego, a nie wyłącznie w charakterze formalnym. Wymaga się, aby dokumentacja była wzajemnie spójna, jednolita terminologicznie, zgodna z zakresem działalności Zamawiającego oraz możliwa do wykorzystania jako podstawa organizacji bezpieczeństwa informacji, cyberbezpieczeństwa, ochrony danych, ciągłości działania i odporności operacyjnej.

Dokumentacja powinna zostać opracowana 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. 2024 poz. 773;
- ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, tekst jednolity Dz.U. 2026 poz. 20, z uwzględnieniem zmian wprowadzonych ustawą z dnia 23 stycznia 2026 r., Dz.U. 2026 poz. 252;
- dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. (NIS2), jako punkt odniesienia dla wymagań dotyczących zarządzania ryzykiem cyberbezpieczeństwa, ciągłości działania, obsługi incydentów, bezpieczeństwa łańcucha dostaw, zarządzania podatnościami, cyberhigieny i nadzoru;
- PN-EN ISO/IEC 27001 – wymagania dla systemu zarządzania bezpieczeństwem informacji;
- PN-EN ISO/IEC 27002 – wytyczne dotyczące stosowania zabezpieczeń bezpieczeństwa informacji;
- PN-EN ISO/IEC 27005 – wytyczne dotyczące zarządzania ryzykiem w bezpieczeństwie informacji;
- PN-EN ISO 22301 – wymagania dla systemu zarządzania ciągłością działania;
- PN-EN ISO 22313 – wytyczne do wdrażania i utrzymania systemu ciągłości działania;
- rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO) oraz ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych;
- aktualne wytyczne i dobre praktyki ENISA dotyczące środków zarządzania ryzykiem cyberbezpieczeństwa oraz odporności sektorów krytycznych.

W ramach realizacji zamówienia Wykonawca zobowiązany będzie do opracowania dokumentacji w taki sposób, aby obejmowała co najmniej:

1. zasady organizacji bezpieczeństwa informacji i cyberbezpieczeństwa u Zamawiającego;
2. zasady zarządzania ryzykiem w obszarze informacji, systemów teleinformatycznych, cyberbezpieczeństwa i ciągłości działania;
3. zasady klasyfikacji informacji, ochrony zasobów informacyjnych i odpowiedzialności za zasoby;
4. zasady ochrony systemów teleinformatycznych, infrastruktury sieciowej, stanowisk roboczych, serwerów, urządzeń mobilnych oraz środowisk IT i OT;
5. zasady ochrony systemów automatyki przemysłowej, telemetryki, zdalnych połączeń technicznych oraz środowisk SCADA, w zakresie adekwatnym do działalności Zamawiającego;
6. zasady zarządzania incydentami bezpieczeństwa informacji, incydentami cyberbezpieczeństwa i naruszeniami ochrony danych osobowych;

7. zasady zapewnienia ciągłości działania w obszarze systemów teleinformatycznych i procesów krytycznych dla świadczenia usług wodociągowo-kanalizacyjnych;
8. zasady tworzenia, testowania, przechowywania i odtwarzania kopii zapasowych;
9. zasady nadzoru nad dostawcami, usługami zewnętrznymi oraz bezpieczeństwem łańcucha dostaw;
10. zasady monitorowania, przeglądów, testów, audytów, działań korygujących i ciągłego doskonalenia;
11. zasady zgodności z wymaganiami KRI, uKSC, RODO, NIS2 oraz wymaganiami normatywnymi wskazanymi przez Zamawiającego.

Opracowana dokumentacja musi:

- być dostosowana do rzeczywistych warunków organizacyjnych i technicznych Zamawiającego;
- uwzględniać specyfikę przedsiębiorstwa wodociągowo-kanalizacyjnego, w tym procesów technologicznych i eksploatacyjnych;
- być oparta na wynikach audytu początkowego oraz zidentyfikowanych ryzykach, lukach i potrzebach organizacji;
- zawierać wzory rejestrów, formularzy, upoważnień, ewidencji, kart, raportów, planów i oświadczeń, tam, gdzie jest to niezbędne do praktycznego stosowania dokumentacji;
- być opracowana w sposób umożliwiający przyjęcie dokumentów do stosowania w drodze właściwych aktów wewnętrznych Zamawiającego;
- zachowywać spójność pomiędzy dokumentami głównymi, procedurami i załącznikami;
- zawierać logiczne powiązanie pomiędzy SZBI, ochroną danych osobowych, zarządzaniem incydentami oraz zarządzaniem ryzykiem;
- uwzględniać podział odpowiedzialności pomiędzy kierownictwo, administratorów, użytkowników, osoby odpowiedzialne za infrastrukturę technologiczną, osoby odpowiedzialne za cyberbezpieczeństwo oraz inne role występujące u Zamawiającego.

Dokumentacja systemowa musi obejmować co najmniej następujące dokumenty główne oraz dokumenty pomocnicze.

1. Polityka Bezpieczeństwa Informacji, w tym w szczególności:

- cele bezpieczeństwa informacji i zasady ich monitorowania;
- opis kontekstu organizacji, interesariuszy oraz czynników wewnętrznych i zewnętrznych;
- zakres SZBI;
- zasady zarządzania dokumentacją systemową;
- role, odpowiedzialności i uprawnienia w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa;
- zasady nadzoru kierownictwa, przeglądów zarządzania i ciągłego doskonalenia;
- zasady klasyfikacji informacji i postępowania z informacjami;
- zasady czystego biurka i czystego ekranu;
- zasady bezpieczeństwa zasobów ludzkich;
- zasady dopuszczania użytkowników do pracy z informacją i systemami;
- zasady zgłaszania oraz obsługi incydentów bezpieczeństwa informacji i cyberbezpieczeństwa;
- zasady monitorowania zgodności z wymaganiami prawnymi, normatywnymi i wewnętrznymi.

2. Polityka Bezpieczeństwa Teleinformatycznego, w tym w szczególności:

- procedura zarządzania dostępem i uprawnieniami;
- procedura uwierzytelniania, stosowania haseł oraz – tam gdzie zasadne – uwierzytelniania wieloskładnikowego;
- procedura bezpieczeństwa sieci teleinformatycznych;

- procedura segmentacji i separacji środowisk IT oraz OT, jeżeli występują;
- procedura użytkowania poczty elektronicznej i korzystania z Internetu;
- procedura bezpiecznej pracy zdalnej;
- procedura korzystania z urządzeń mobilnych i nośników przenośnych;
- procedura szyfrowania danych oraz zasad stosowania kryptografii;
- procedura wykonywania, przechowywania, testowania i odtwarzania kopii zapasowych;
- procedura monitorowania, rejestrowania zdarzeń oraz przeglądu logów;
- procedura zarządzania podatnościami, aktualizacjami i poprawkami bezpieczeństwa;
- procedura zarządzania zmianą w systemach teleinformatycznych;
- procedura przeglądów i konserwacji systemów teleinformatycznych;
- procedura ponownego wykorzystania, przekazania i bezpiecznej utylizacji nośników danych;
- ewidencja sprzętu, oprogramowania, zasobów teleinformatycznych i kont uprzywilejowanych;
- wzory raportów administratora lub osoby odpowiedzialnej za utrzymanie systemów;
- rejestr użytkowników połączeń zdalnych, w tym VPN, jeżeli jest stosowany.

3. Polityka Bezpieczeństwa Fizycznego i Środowiskowego, w tym w szczególności:

- zasady ochrony fizycznej budynków, pomieszczeń i stref;
- procedura zarządzania kluczami, kartami dostępu, kodami i innymi środkami wejścia;
- wykaz pomieszczeń lub części pomieszczeń stanowiących obszar przetwarzania informacji;
- zasady dostępu do serwerowni, punktów dystrybucyjnych, sterowni, pomieszczeń technicznych i innych obszarów wrażliwych;
- ewidencja osób upoważnionych do przebywania w zabezpieczonych obszarach;
- zasady ochrony urządzeń, infrastruktury krytycznej i zasobów technicznych przed uszkodzeniem, utratą, sabotażem lub nieuprawnionym dostępem;
- procedura postępowania w zabezpieczonych obszarach;
- zasady nadzoru nad gośćmi, serwisantami i podmiotami zewnętrznymi;
- zasady reagowania na zdarzenia fizyczne wpływające na bezpieczeństwo informacji i ciągłość działania.

4. Polityka Ochrony Danych Osobowych, w tym w szczególności:

- zasady przetwarzania danych osobowych zgodnie z RODO i ustawą o ochronie danych osobowych;
- zasady realizacji obowiązków administratora;
- zasady nadawania, zmiany i cofania upoważnień do przetwarzania danych osobowych;
- ewidencja osób upoważnionych do przetwarzania danych osobowych;
- oświadczenia o zachowaniu poufności;
- wzory rejestrów udostępnień danych osobowych, jeżeli są stosowane;
- wzory umów powierzenia przetwarzania danych osobowych i wykaz tych umów;
- wzory dokumentów związanych z realizacją praw osób, których dane dotyczą;
- rejestr realizacji żądań osób, których dane dotyczą;
- wzór rejestru czynności przetwarzania oraz – jeżeli zasadne – rejestru kategorii czynności przetwarzania;
- metodologia szacowania ryzyka dla ochrony danych osobowych, zintegrowana z ryzykiem bezpieczeństwa informacji i cyberbezpieczeństwa;
- procedura postępowania w przypadku naruszenia ochrony danych osobowych;
- wzory dokumentów pomocniczych dotyczących analizy naruszeń, zgłoszeń i oceny ryzyka;
- wzór raportu z audytu zgodności z RODO, jeżeli Zamawiający wymaga takiego dokumentu w ramach dokumentacji systemowej.

5. Dokumentacja zarządzania ryzykiem, w tym w szczególności:

- metodyka szacowania ryzyka dla bezpieczeństwa informacji, cyberbezpieczeństwa, ciągłości działania oraz – jeśli Zamawiający tego wymaga – ochrony danych osobowych;
- kryteria oceny prawdopodobieństwa, skutku, poziomu ryzyka i akceptacji ryzyka;
- zasady postępowania z ryzykiem;

- wzory kart ryzyka, rejestru ryzyk, planów postępowania z ryzykiem i przeglądów ryzyka;
- powiązanie wyników analizy ryzyka z doborem zabezpieczeń i dokumentacją SZBI.

Wymagania wobec sposobu realizacji usługi:

Wykonawca zobowiązany jest do realizacji usługi z należytą starannością, w sposób uwzględniający wyniki audytu początkowego, rzeczywiste potrzeby Zamawiającego oraz specyfikę działalności Zamawiającego.

Wykonawca zobowiązany jest do:

- analizy dokumentacji wejściowej Zamawiającego;
- uwzględnienia istniejących rozwiązań organizacyjnych i technicznych;
- dostosowania dokumentacji do struktury organizacyjnej Zamawiającego;
- uwzględnienia obowiązków wynikających z KRI, uKSC, RODO oraz wymagań wynikających z NIS2 jako punktu odniesienia dojrzałościowego i organizacyjnego;
- zapewnienia spójności pomiędzy dokumentacją SZBI, ochroną danych osobowych, zarządzaniem incydentami i analizą ryzyka;
- przekazania dokumentów w formie umożliwiającej ich zatwierdzenie i wdrożenie przez Zamawiającego.

Zamawiający wymaga, aby dokumentacja uwzględniała zarówno wymagania systemowe, jak i specyfikę branży wodociągowo-kanalizacyjnej, w tym potrzebę zapewnienia ciągłości świadczenia usług publicznych, ochrony infrastruktury technicznej, bezpieczeństwa procesów technologicznych, bezpieczeństwa dostępu zdalnego, bezpieczeństwa dostawców oraz odporności na zakłócenia i incydenty mogące wpływać na funkcjonowanie przedsiębiorstwa. Sektor krytyczny i branżowy kontekst takiego podejścia są szeroko akcentowane w materiałach ENISA dotyczących cyberbezpieczeństwa sektorów krytycznych

Zamawiający dopuszcza możliwość realizacji usługi w formie zdalnej.

2. Szkolenie z zakresu cyberbezpieczeństwa dla kadry kierowniczej z zakresu wdrażanego Systemu Zarządzania Bezpieczeństwem Informacji

Przedmiotem zamówienia jest realizacja szkolenia z zakresu cyberbezpieczeństwa przeznaczonego dla kadry zarządzającej, osób odpowiedzialnych za bezpieczeństwo informacji, cyberbezpieczeństwo, ciągłość działania, IT, OT/ICS oraz osób pełniących funkcje decyzyjne i nadzorcze u Zamawiającego.

Celem szkolenia jest zapewnienie właściwego zrozumienia, wdrożenia oraz nadzoru nad dokumentacją Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), a także budowanie kompetencji w zakresie zarządzania bezpieczeństwem informacji i cyberbezpieczeństwem w kontekście działalności przedsiębiorstwa wodociągowo-kanalizacyjnego.

Szkolenie powinno uwzględniać specyfikę organizacji, w tym środowisk IT, OT/ICS/SCADA oraz znaczenie ciągłości działania procesów technologicznych.

Minimalny zakres szkolenia powinien obejmować co najmniej:

1. Wprowadzenie do SZBI - omówienie roli systemów zarządzania bezpieczeństwem informacji i ciągłością działania w organizacji oraz ich znaczenia dla funkcjonowania przedsiębiorstwa wodociągowo-kanalizacyjnego.
2. Podstawy prawne i normatywne - przegląd wymagań wynikających z KRI, ustawy o krajowym systemie cyberbezpieczeństwa, RODO oraz odniesienie do wymagań NIS2 i norm ISO (27001, 27002, 27005, 22301).
3. Polityka bezpieczeństwa informacji i struktura dokumentacji SZBI - omówienie kluczowych dokumentów systemowych (PBI, PBT, PBF, procedury), ich roli, zakresu oraz zasad stosowania w organizacji.
4. System zarządzania ciągłością działania (SZCD) - zasady identyfikacji procesów krytycznych, planów ciągłości działania, procedur awaryjnych oraz roli kadry w zapewnieniu ciągłości funkcjonowania organizacji.
5. Zarządzanie ryzykiem - zasady identyfikacji, analizy i oceny ryzyka w obszarze bezpieczeństwa informacji, cyberbezpieczeństwa oraz ciągłości działania, w tym rola kierownictwa w procesie akceptacji ryzyka.
6. Role i odpowiedzialności w SZBI i SZCD - obowiązki kierownictwa, administratorów, użytkowników oraz osób odpowiedzialnych za IT, OT i bezpieczeństwo informacji.
7. Zarządzanie incydentami i naruszeniami - zasady zgłaszania, obsługi i nadzoru nad incydentami bezpieczeństwa informacji, cyberbezpieczeństwa oraz naruszeniami ochrony danych osobowych.
8. Bezpieczeństwo środowisk IT/OT/ICS w ujęciu zarządczym - kluczowe ryzyka dla infrastruktury technicznej, znaczenie separacji IT/OT, nadzoru nad dostępem oraz bezpieczeństwa usług zewnętrznych.
9. Nadzór nad dokumentacją i zgodnością - zasady przeglądów, audytów, monitorowania zgodności oraz ciągłego doskonalenia SZBI i SZCD.
10. Budowanie świadomości i kultury bezpieczeństwa - znaczenie szkoleń, komunikacji wewnętrznej oraz zaangażowania kadry zarządzającej w utrzymanie skutecznego systemu bezpieczeństwa.

Wymagania dotyczące realizacji szkolenia

Zamawiający wymaga, aby szkolenie:

- było bezpośrednio powiązane z opracowaną dokumentacją SZBI u Zamawiającego;
- miało charakter praktyczny i odnosiło się do rzeczywistych procesów i ryzyk występujących w organizacji;
- uwzględniało przykłady sytuacji decyzyjnych, incydentów oraz odpowiedzialności kadry zarządzającej;

- wspierało wdrożenie i stosowanie dokumentacji systemowej w praktyce;
- zostało przeprowadzone w sposób umożliwiający aktywny udział uczestników (np. dyskusja, omówienie przypadków).

Szkolenie powinno stanowić integralny element wdrożenia SZBI oraz wspierać Zamawiającego w osiągnięciu zgodności z wymaganiami KRI, uKSC oraz dobrymi praktykami wynikającymi z norm ISO i dyrektywy NIS2.

Zamawiający wymaga przeprowadzenia szkolenia w wymiarze nie krótszym niż **3 godziny zegarowe** dla jednej grupy uczestników **(łączna ilość osób: 7).**

Zamawiający wymaga, aby szkolenie zostało zrealizowane w formie stacjonarnej, zaś po ukończeniu szkolenia przez uczestników wymagane jest wydanie stosownych certyfikatów potwierdzających udział w szkoleniu.

3. Audyt końcowy obejmujący zgodność z KRI, uoKSC oraz SZBI

Przedmiotem zamówienia jest wykonanie kompleksowej usługi audytorskiej obejmującej:

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

Audyty mają charakter **audytu końcowego** realizowanego w ramach projektu grantowego „Cyberbezpieczne Wodociągi" i mają służyć ocenie stanu docelowego bezpieczeństwa organizacji po realizacji działań przewidzianych w projekcie, ocenie skuteczności zastosowanych środków organizacyjnych i technicznych oraz potwierdzeniu poziomu zgodności Zamawiającego z wymaganiami dotyczącymi bezpieczeństwa informacji, cyberbezpieczeństwa i ciągłości działania. W związku z powyższym audyt powinien zostać przeprowadzony na końcu realizacji projektu przez Zamawiającego, tj. po realizacji wszystkich dostaw z zakresu cyberbezpieczeństwa, a także po opracowaniu dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.

Zakres audytu musi uwzględniać specyfikę działalności przedsiębiorstwa wodociągowo-kanalizacyjnego, w tym środowisk IT i OT, systemów sterowania, automatyki przemysłowej, systemów telemetrycznych, systemów SCADA, systemów zdalnego monitoringu i infrastruktury krytycznej lub mającej istotne znaczenie dla ciągłości świadczenia usług zbiorowego zaopatrzenia w wodę i odprowadzania ścieków.

Audyty mają zostać przeprowadzone w oparciu o aktualnie obowiązujące oraz mające zastosowanie przepisy prawa, normy, wytyczne i dobre praktyki, w szczególności:

- rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności (KRI), Dz.U. 2024 poz. 773;
- ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, tekst jednolity Dz.U. 2026 poz. 20, z uwzględnieniem zmian wprowadzonych ustawą z dnia 23 stycznia 2026 r., Dz.U. 2026 poz. 252;
- dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. (NIS2), jako punkt odniesienia dla oceny dojrzałości organizacyjnej i technicznej 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 – wytyczne dotyczące stosowania zabezpieczeń bezpieczeństwa informacji;
- PN-EN ISO/IEC 27005 – wytyczne dotyczące zarządzania ryzykiem w bezpieczeństwie informacji;
- PN-EN ISO 22301 – wymagania dla systemu zarządzania ciągłością działania;
- PN-EN ISO 22313 – wytyczne do wdrażania i utrzymania systemu ciągłości działania;
- aktualne wytyczne i dobre praktyki ENISA dotyczące środków zarządzania ryzykiem cyberbezpieczeństwa, wdrażania wymagań NIS2 oraz bezpieczeństwa łańcucha dostaw.

W ramach realizacji zamówienia Wykonawca zobowiązany będzie co najmniej do:

1. przeprowadzenia analizy dokumentacji Zamawiającego, w tym dokumentacji opracowanej, wdrożonej lub zaktualizowanej w toku realizacji projektu, w szczególności polityk, procedur, instrukcji, rejestrów, planów, analiz ryzyka, planów ciągłości działania, planów odtworzeniowych, dokumentacji technicznej, dokumentacji systemów teleinformatycznych oraz dokumentacji dotyczącej środowisk OT/ICS/SCADA;
2. przeprowadzenia wywiadów i warsztatów z przedstawicielami Zamawiającego, w tym z kierownictwem, personelem odpowiedzialnym za IT, OT, cyberbezpieczeństwo, utrzymanie ruchu, automatykę, eksploatację sieci, ochronę danych, zarządzanie kryzysowe i ciągłość działania;
3. przeprowadzenia oceny dojrzałości SZBI, 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;

4. przeprowadzenia 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;
5. przeprowadzenia oceny zgodności z wymaganiami wynikającymi z ustawy o krajowym systemie cyberbezpieczeństwa, w tym w zakresie organizacji systemu bezpieczeństwa, zarządzania incydentami, środków bezpieczeństwa, nadzoru, dokumentowania działań oraz gotowości do spełniania obowiązków podmiotów objętych regulacją;
6. przeprowadzenia oceny zgodności i dojrzałości względem wymagań NIS2, w szczególności w obszarze:

   - polityk analizy ryzyka i bezpieczeństwa systemów informacyjnych,
   - obsługi incydentów,
   - ciągłości działania, backupu i disaster recovery,
   - 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;

7. przeprowadzenia oceny obszarów branżowych 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 telemetryki, 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;

8. weryfikacji oraz oceny skuteczności wdrożonych działań naprawczych, organizacyjnych i technicznych;
9. oceny, czy wdrożone rozwiązania przyczyniły się do podniesienia poziomu bezpieczeństwa, odporności operacyjnej i ciągłości działania Zamawiającego;

10. identyfikacji niezgodności, luk, ryzyk resztkowych, podatności organizacyjnych i technicznych oraz obszarów wymagających dalszych działań doskonalących;
11. opracowania raportu końcowego z audytu końcowego.

Minimalne wymagania dotyczące raportu końcowego z audytu końcowego

Raport końcowy z audytu musi zawierać co najmniej:

1. opis celu, zakresu i metodyki audytu;
2. opis stanu istniejącego na dzień zakończenia realizacji audytu;
3. ocenę zgodności z wymaganiami KRI, uoKSC, NIS2 oraz wskazanymi normami;
4. ocenę dojrzałości SZBI,
5. ocenę stopnia wdrożenia zaleceń wynikających z audytu początkowego;
6. identyfikację pozostających luk, niezgodności, słabości i ryzyk;
7. ocenę wpływu wdrożonych rozwiązań na bezpieczeństwo świadczenia usług wodociągowo-kanalizacyjnych;
8. ocenę skuteczności wdrożonych działań naprawczych, usprawniających i rozwojowych;
9. wskazanie ryzyk resztkowych oraz obszarów wymagających dalszego doskonalenia;
10. macierz zgodności lub tabelę odniesień do wymagań prawnych, normatywnych i branżowych;
11. podsumowanie dla kierownictwa w formie syntetycznej, umożliwiające ocenę osiągniętego poziomu zgodności i podjęcie dalszych decyzji zarządczych.

Raport powinien być sporządzony w sposób praktyczny i wdrożeniowy, tak aby stanowił potwierdzenie osiągniętych efektów projektu, podstawę do odbioru rezultatów działań zrealizowanych w ramach projektu poprawy cyberbezpieczeństwa oraz materiał służący do dalszego utrzymania, monitorowania i doskonalenia systemów bezpieczeństwa informacji i ciągłości działania.

Wymagania wobec sposobu realizacji usługi

Wykonawca zobowiązany jest przeprowadzić audyt z należytą starannością, w sposób niezależny, obiektywny i zapewniający poufność informacji pozyskanych w toku realizacji zamówienia. Wykonawca powinien dysponować personelem posiadającym doświadczenie w audytach bezpieczeństwa informacji, cyberbezpieczeństwa, ciągłości działania oraz – co najmniej w zakresie zespołu realizującego – doświadczenie w audytach środowisk przemysłowych lub infrastruktury krytycznej, usług kluczowych albo sektorów komunalnych.

Zamawiający wymaga, aby wnioski z audytu uwzględniały zarówno ogólne wymagania systemowe, jak i specyfikę branży wodociągowo-kanalizacyjnej, w tym konieczność zapewnienia ciągłości świadczenia usług publicznych, bezpieczeństwa procesów technologicznych, niezawodności infrastruktury oraz ochrony danych i systemów wykorzystywanych w eksploatacji sieci wodociągowej i kanalizacyjnej.

Zamawiający wymaga przeprowadzenia audytu w formie stacjonarnej. Jedynie w przypadku konieczności uzupełnień, dopuszczalna jest forma zdalna.

Zamawiający wymaga, aby Wykonawca opracował i przedłożył raport w wersji papierowej i elektronicznej. Raport z audytu powinien być podpisany przez audytora opracowującego audyt. Zamawiający zastrzega prawo do wniesienia uwag do przedłożonej dokumentacji, a Wykonawca zobowiązuje się do jej skorygowania i uwzględnienia wniesionych uwag.