Cyberbezpieczne Wodociągi

ZAŁĄCZNIK NR 2 – Opis Przedmiotu Zamówienia (OPZ)

Opis Przedmiotu Zamówienia

Audyt Systemu Zarządzania Bezpieczeństwem Informacji oraz audyt cyberbezpieczeństwa sieci IT/OT/ICS/IIoT

Spis treści

Informacje ogólne1

CHARAKTERYSTYKA ŚRODOWISKA OBJĘTEGO AUDYTEM 2

CZĘŚĆ A – AUDYT SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI 3

CZĘŚĆ B – AUDYT CYBERBEZPIECZEŃSTWA SIECI IT/OT/ICS/IIOT 5

POSTANOWIENIA WSPÓLNE 7

Informacje ogólne

Niniejszy Opis Przedmiotu Zamówienia (OPZ) stanowi podstawę do przeprowadzenia postępowania zakupowego w ramach projektu grantowego „Cyberbezpieczne wodociągi na terenie gminy Środa Wielkopolska", realizowanego przez Miejskie Przedsiębiorstwo Energetyki Cieplnej, Wodociągów i Kanalizacji Sp. z o.o. w Środzie Wielkopolskiej (dalej: Zamawiający).

Projekt jest współfinansowany ze środków Krajowego Planu Odbudowy i Zwiększania Odporności (KPO), w ramach inwestycji C3.1.1 CyberPL (priorytet C3 – Cyberbezpieczeństwo), na podstawie umowy o powierzenie grantu nr KPOD.05.10-CW.01-001/25/0377/KPOD.05.10-CW.01-001/25/2026.

Cyberbezpieczne Wodociągi

Kody CPV: 79212000-3 Usługi audytu; 72810000-1 Usługi audytu komputerowego; 72150000-1 Usługi doradztwa w zakresie audytu komputerowego.

Przedmiot zamówienia obejmuje dwie części:

1. **Część A** – audyt Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) (kategoria kosztów KPO: U25).
2. **Część B** – audyt cyberbezpieczeństwa sieci IT/OT/ICS/IIoT (kategoria kosztów KPO: U37).

Wykonawca składa ofertę na obie części łącznie. Każda część stanowi odrębny produkt, rozliczany na podstawie odrębnej faktury.

Termin realizacji całości przedmiotu zamówienia: **do dnia 29.12.2026 r.**

Charakterystyka środowiska objętego audytem

Audyty obejmują stan organizacji i infrastruktury Zamawiającego po zakończeniu wdrożenia realizowanego w ramach projektu grantowego. Poniższe dane mają charakter orientacyjny; szczegółowe informacje (inwentaryzacja aktywów, dokumentacja powykonawcza, dokumentacja SZBI) zostaną przekazane Wykonawcy po podpisaniu umowy, z zachowaniem poufności.

Organizacja

- Przedsiębiorstwo wodociągowo-kanalizacyjne i ciepłownicze, ok. 90 pracowników, w tym kilkunastu pracowników obsługujących systemy IT/OT.
- Siedziba Zamawiającego oraz kilka obiektów technicznych (stacje uzdatniania wody, oczyszczalnia ścieków, przepompownie, źródło ciepła) połączonych z siedzibą łączami WAN/VPN.
- Wdrożony w ramach projektu System Zarządzania Bezpieczeństwem Informacji (dokumentacja: polityki, procedury, analiza ryzyka, deklaracja stosowania, plany ciągłości działania, rejestry).
- Zrealizowany w ramach projektu program szkoleń z zakresu cyberbezpieczeństwa (pracownicy, kadra zarządzająca, personel IT).

Infrastruktura IT (stan po wdrożeniu)

- Domena Active Directory, ok. 100 stacji roboczych i urządzeń końcowych objętych ochroną antywirusową; do 200 urządzeń końcowych objętych kontrolą dostępu do sieci (NAC).
- Firewall nowej generacji (NGFW) w konfiguracji redundantnej (2 urządzenia) z funkcjami UTM i ochrony sieci OT; 4 firewalle w lokalizacjach zdalnych; 5 zarządzalnych przełączników dostępowych z obsługą 802.1X; punkt dostępowy WiFi.

- Klaster serwerów (wirtualizacja) dla systemów bezpieczeństwa i systemów dziedzinowych; dedykowany serwer kopii zapasowych; platforma NAS do odmiejscowienia kopii zapasowych.
- Systemy bezpieczeństwa: SIEM, NAC, MFA, klient VPN z zarządzaniem punktami końcowymi (EMS), system zarządzania dostępem uprzywilejowanym (PAM), system monitorowania infrastruktury, system ITSM.

Infrastruktura OT (stan po wdrożeniu)

- System SCADA nadzorujący procesy technologiczne (uzdatnianie i dystrybucja wody, oczyszczanie ścieków, ciepłownictwo), sterowniki PLC i panele HMI w obiektach technicznych, komunikacja z wykorzystaniem protokołów przemysłowych.
- Segmentacja sieci IT/OT zrealizowana na poziomie NGFW zgodnie z modelem Purdue (poziomy 2–4).
- 4 sprzętowe sondy do pasywnego monitorowania ruchu w sieci OT (analiza protokołów przemysłowych).
- System monitorowania infrastruktury OT.
- Zdalny dostęp serwisowy do OT realizowany przez VPN z uwierzytelnianiem wieloskładnikowym i system PAM.

Część A – Audyt Systemu Zarządzania Bezpieczeństwem Informacji

Cel

Niezależna ocena wdrożonego SZBI pod kątem jego skuteczności, zgodności z wymaganiami prawnymi i normatywnymi oraz adekwatności do potrzeb i profilu ryzyka Zamawiającego. Wyniki audytu posłużą do doskonalenia SZBI.

Kryteria audytu

1. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (uKSC) w brzmieniu obowiązującym w dniu realizacji audytu, wraz z aktami wykonawczymi – w zakresie obowiązków podmiotu krajowego systemu cyberbezpieczeństwa właściwych dla Zamawiającego, w szczególności dotyczących systemu zarządzania bezpieczeństwem informacji, zarządzania ryzykiem, obsługi incydentów i ciągłości działania.
2. Norma PN-EN ISO/IEC 27001:2023 – w zakresie, w jakim wymagania normy są adekwatne do wdrożonego SZBI i stanowią punkt odniesienia dla oceny kompletności i skuteczności systemu (w tym zabezpieczenia z Załącznika A normy w zakresie objętym deklaracją stosowania Zamawiającego).

3. Dokumentacja SZBI Zamawiającego (polityki, procedury, instrukcje) – w zakresie zgodności stanu faktycznego z przyjętymi regulacjami wewnętrznymi.

Zakres

Audyt obejmuje co najmniej następujące obszary:

1. Kontekst organizacji, zakres SZBI, role i odpowiedzialności, zaangażowanie kierownictwa.
2. Polityka bezpieczeństwa informacji oraz polityki i procedury szczegółowe – kompletność, spójność, aktualność, znajomość wśród pracowników.
3. Szacowanie i postępowanie z ryzykiem – metodyka, rejestr ryzyk, plan postępowania z ryzykiem, powiązanie z wdrożonymi zabezpieczeniami.
4. Deklaracja stosowania (SoA) – uzasadnienie włączeń i wyłączeń, zgodność ze stanem wdrożenia.
5. Zarządzanie aktywami – inwentaryzacja aktywów IT/OT, klasyfikacja informacji, właścicielstwo aktywów.
6. Zarządzanie incydentami bezpieczeństwa – procedury wykrywania, obsługi, eskalacji i raportowania incydentów, w tym obowiązki zgłaszania wynikające z uKSC; rejestr incydentów.
7. Ciągłość działania i odtwarzanie po awarii (BCP/DRP) – plany, kopie zapasowe, testy odtwarzania, ciągłość procesów technologicznych OT.
8. Bezpieczeństwo łańcucha dostaw i relacje z dostawcami – umowy, wymagania bezpieczeństwa wobec dostawców, nadzór nad dostępem serwisowym.
9. Bezpieczeństwo zasobów ludzkich – szkolenia i budowanie świadomości, zasady dostępu w cyklu zatrudnienia.
10. Kontrola dostępu i zarządzanie tożsamością – zasady nadawania, przeglądu i odbierania uprawnień, konta uprzywilejowane.
11. Bezpieczeństwo fizyczne i środowiskowe obiektów przetwarzania (serwerownia, obiekty technologiczne).
12. Monitorowanie, pomiary, audyty wewnętrzne i przeglądy zarządcze SZBI; działania korygujące.
13. Zgodność dokumentacji SZBI ze stanem faktycznym – weryfikacja wybranych zabezpieczeń na podstawie dowodów (próbkowanie).

Produkty

1. Raport z audytu SZBI zawierający co najmniej: cel, zakres i kryteria audytu; opis badanych obszarów; ustalenia z klasyfikacją (niezgodność duża / niezgodność mała / obserwacja / możliwość doskonalenia) wraz z dowodami; ocenę ogólną skuteczności SZBI.
2. Mapę zgodności – zestawienie wymagań uKSC oraz wymagań PN-EN ISO/IEC 27001:2023 (rozdziały 4–10 i Załącznik A w zakresie SoA) ze wskazaniem stopnia spełnienia każdego wymagania.

3. Ocenę dojrzałości SZBI w poszczególnych obszarach (skala ustalona z Zamawiającym).
4. Plan działań korygujących i doskonalących – lista zaleceń z priorytetem, proponowanym terminem realizacji i wskazaniem odpowiedzialności.
5. Streszczenie zarządcze oraz prezentację wyników dla kierownictwa Zamawiającego.

Część B – Audyt cyberbezpieczeństwa sieci IT/OT/ICS/IIoT

Cel

Ocena stanu technicznego i organizacyjnego zabezpieczeń sieci i systemów IT oraz OT/ICS/IIoT Zamawiającego po wdrożeniu, identyfikacja podatności oraz ryzyk związanych z funkcjonowaniem systemów informatycznych i przemysłowych, wraz z rekomendacjami środków ochrony.

Zakres – obszar IT

1. Architektura sieci i segmentacja – zgodność z modelem Purdue (poziomy 2–4), separacja IT/OT, strefy i kanały komunikacji, reguły ruchu między segmentami.
2. Firewalle NGFW i firewalle lokalizacji zdalnych – polityki bezpieczeństwa, reguły zbędne i nadmiarowe, IPS, sygnatury OT, filtrowanie aplikacji i WWW, logowanie, konfiguracja HA, aktualność firmware.
3. Przełączniki i sieć dostępowa – konfiguracja VLAN, 802.1X, zabezpieczenia warstwy 2, zarządzanie urządzeniami, sieć WiFi.
4. Kontrola dostępu do sieci (NAC) – polityki, profilowanie urządzeń, obsługa urządzeń niezgodnych i gości.
5. Zdalny dostęp – VPN, uwierzytelnianie wieloskładnikowe, polityki EMS, dostęp dostawców i serwisu.
6. Usługi katalogowe (Active Directory) – hardening, polityki GPO, model warstwowy kont uprzywilejowanych, polityki haseł, konta nieużywane i serwisowe, delegacje.
7. Serwery i wirtualizacja – hardening systemów operacyjnych i hypervisora, aktualizacje, usługi zbędne, konfiguracja klastra.
8. Kopie zapasowe – polityka kopii (w tym zasada 3-2-1), zakres (w tym systemy OT), odmiejscowienie, ochrona kopii przed modyfikacją, **test odtworzenia wybranego systemu**.
9. SIEM – kompletność źródeł logów (IT i OT), reguły korelacji i alarmowania, retencja, obsługa alertów.
10. Zarządzanie dostępem uprzywilejowanym (PAM) – objęcie kont i systemów, rejestracja sesji, zasady udzielania dostępu.
11. Stacje robocze – ochrona antywirusowa/EDR, uprawnienia lokalne, szyfrowanie, aktualizacje.
12. Ekspozycja zewnętrzna – adresacja publiczna Zamawiającego, usługi wystawione do Internetu.

Cyberbezpieczne Wodociągi

Zakres – obszar OT/ICS/IIoT

1. Inwentaryzacja aktywów OT (sterowniki PLC, panele HMI, serwery SCADA, urządzenia sieciowe, urządzenia IIoT) – weryfikacja zgodności inwentaryzacji ze stanem faktycznym.
2. System SCADA i stacje inżynierskie – hardening, konta i uprawnienia, aktualizacje, dostęp zdalny, kopie konfiguracji.
3. Sterowniki PLC i panele HMI – wersje firmware, zabezpieczenie dostępu (hasła, tryby pracy, blokady zapisu), kopie programów, dostęp fizyczny.
4. Protokoły przemysłowe i komunikacja – analiza ruchu w sieci OT, komunikacja nieautoryzowana lub niezabezpieczona, komunikacja OT–IT oraz OT–Internet.
5. Zdalny dostęp do OT – ścieżki dostępu serwisowego, uwierzytelnianie, nadzór nad sesjami, dostęp producentów i integratorów.
6. Sondy monitorowania OT – rozmieszczenie, pokrycie segmentów, konfiguracja alarmowania, integracja z SIEM.
7. Odporność procesów technologicznych – tryby pracy awaryjnej, zależność procesów od systemów IT, procedury pracy ręcznej.

Techniki badania i zasady realizacji

1. Przegląd konfiguracji urządzeń i systemów w odniesieniu do dobrych praktyk (CIS Benchmarks, zalecenia producentów, IEC 62443 dla obszaru OT).
2. Autoryzowany skan podatności w obszarze IT (serwery, stacje robocze, urządzenia sieciowe, usługi) – z uzgodnieniem okien czasowych i zakresu adresacji.
3. Test ekspozycji zewnętrznej – skan i weryfikacja manualna usług dostępnych z Internetu dla adresacji publicznej Zamawiającego.
4. W obszarze OT – **wyłącznie metody pasywne** (analiza ruchu, dane z sond, przegląd konfiguracji, oględziny) oraz przegląd manualny; aktywne skanowanie urządzeń OT dopuszczalne wyłącznie na podstawie odrębnej, pisemnej zgody Zamawiającego, dla wskazanych urządzeń i w uzgodnionym oknie serwisowym.
5. Wywiady z personelem IT/OT oraz przegląd dokumentacji powykonawczej wdrożenia.
6. Zamówienie nie obejmuje pełnych testów penetracyjnych z eksploatacją podatności; weryfikacja manualna ogranicza się do potwierdzenia istnienia podatności bez działań mogących zakłócić pracę systemów.
7. Zasady zaangażowania: zakaz testów odmowy usługi (DoS), zakaz działań mogących wpłynąć na procesy technologiczne, uzgodnione okna czasowe, osoby kontaktowe po obu stronach, procedura natychmiastowego przerwania prac, zobowiązanie do poufności oraz trwałe usunięcie danych Zamawiającego po zakończeniu audytu.

Cyberbezpieczne Wodociągi

Produkty

1. Raport techniczny z audytu zawierający co najmniej: zakres i metody badania; opis stanu architektury i zabezpieczeń; listę zidentyfikowanych podatności i słabości konfiguracyjnych z oceną istotności (CVSS lub równoważna skala), dowodami oraz dotkniętymi aktywami; rekomendacje usunięcia z priorytetyzacją.
2. Surowe wyniki skanów podatności i analiz ruchu (w formacie elektronicznym umożliwiającym dalsze przetwarzanie).
3. Zestawienie ryzyk dla obszaru OT z odniesieniem do wpływu na procesy technologiczne.
4. Streszczenie zarządcze oraz prezentację wyników dla kierownictwa Zamawiającego.
5. Retest podatności sklasyfikowanych jako krytyczne i wysokie po ich usunięciu przez Zamawiającego – jednorazowo, w terminie uzgodnionym z Zamawiającym, nie później niż 30 dni od przekazania raportu końcowego; wynik retestu w formie uzupełnienia raportu.

Postanowienia wspólne

1. Wszystkie produkty przekazywane są w języku polskim, w formie elektronicznej (PDF oraz format edytowalny), raporty końcowe dodatkowo podpisane kwalifikowanym podpisem elektronicznym lub w formie papierowej.
2. Wykonawca zobowiązany jest do zachowania w poufności wszelkich informacji uzyskanych w związku z realizacją zamówienia, w tym po jego zakończeniu, oraz do zawarcia umowy o zachowaniu poufności przed uzyskaniem dostępu do dokumentacji i systemów.
3. Wykonawca przenosi na Zamawiającego autorskie prawa majątkowe do raportów i pozostałych produktów na wszystkich polach eksploatacji niezbędnych do ich wykorzystania, w tym do udostępnienia instytucjom kontrolującym realizację projektu grantowego.
4. Wykonawca zapewni przetwarzanie danych osobowych zgodnie z RODO oraz zawrze z Zamawiającym umowę powierzenia przetwarzania danych, o ile będzie to wymagane.
5. Produkty muszą zawierać oznaczenia wymagane dla projektów współfinansowanych z KPO.