Załącznik nr 2 do zaproszenia do złożenia oferty

Opis przedmiotu zamówienia

Numer postępowania ADM.018.2026.11.AS

Opracowanie dokumentacji SZBI i SZCD oraz planów BCP i DRP i wprowadzenie procedur

Przedsiębiorstwo Usług Komunalnych „PEKO” sp. z o.o. w Kosakowie,

ul. Chrzanowskiego 44,

81-198 Kosakowo,

NIP 9581154984,

REGON 191416896,

KRS 0000038875.

Zamówienie w projekcie „Kompleksowa rozbudowa i modernizacja rozwiązań z zakresu cyberbezpieczeństwa w PUK PEKO”, program „Cyberbezpieczne Wodociągi”, inwestycja C3.1.1 KPO.

1. Przedmiot umowy

Wykonawca opracuje i uzupełni pełną, spójną dokumentację Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), Systemu Zarządzania Ciągłością Działania (SZCD), plany ciągłości działania (BCP) i odtwarzania po awarii (DRP) i przygotuje je do przyjęcia przez PUK „PEKO”. Dokumenty mają nadawać się do codziennego użycia w działalności wodociągowej, kanalizacyjnej, PSZOK i utrzymania czystości w gminie, z uwzględnieniem systemów informatycznych IT i przemysłowych OT.

Spółka udostępni posiadane materiały wskazane w załączniku nr 2B. Obejmują one dokumenty opracowane i stosowane, dokumenty opracowane, lecz jeszcze niewprowadzone, oraz obszary wymagające opracowania lub uzupełnienia. Status „Gotowe” oznacza dokument opracowany i wdrożony przez PUK „PEKO”. Wykonawca weryfikuje również dokumenty o tym statusie.

Wykonawca w ramach zamówienia zweryfikuje aktualność, kompletność, spójność, stan stosowania i dostosowanie materiałów do PUK „PEKO” oraz zakresu D1–D3. Wykorzysta prawidłowe treści, zaktualizuje lub uzupełni wymagające zmian, a brakujące opracuje. Rezultatem będzie pełny, spójny pakiet dokumentacji w granicach OPZ, mający odzwierciedlenie w funkcjonowaniu Spółki. Wszystkie te prace mieszczą się w cenie ryczałtowej.

Nowe i zmieniane dokumenty muszą być kompatybilne z wymaganiami i procedurami obowiązującymi w Spółce, w szczególności z PODO, PBI, dokumentacją IT/OT, instrukcjami eksploatacyjnymi i planami ciągłości. Kompatybilność obejmuje wspólne definicje, zakresy, identyfikatory i wersje, właścicieli i zastępstwa, uprawnienia, kontakty, progi i ścieżki eskalacji, terminy zgłoszeń, formularze, rejestry oraz wzajemne odwołania. Wykonawca wskaże kolizje i zaproponuje ich usunięcie. Zmianę obowiązujących zasad zatwierdza PUK „PEKO”. Nie wolno zastępować prawidłowych dokumentów ogólnym szablonem bez wykazania potrzeby i uzgodnienia zmiany.

2. Zakres i wycena

Pozycja	Wymagany zakres
D1 Dokumentacja SZBI	Zakres systemu, procesy i aktywa z właścicielami, klasyfikacja informacji, role i zastępstwa, analiza i rejestr ryzyka, postępowanie z ryzykiem oraz brakujące lub wymagające dostosowania procedury i rejestry.
D2 Plany BCP i DRP	Plan postępowania podczas awarii, ciągłości usług i odtwarzania krytycznych systemów. Scenariusze, karty działań, kolejność przywracania, zasoby, kontakty, walidacja i dostęp offline.
D3 Dokumentacja SZCD	Zasady zarządzania ciągłością, analiza wpływu na działalność BIA, ryzyka zakłóceń, strategie, odpowiedzialność oraz plan przyszłych przeglądów, ćwiczeń i aktualizacji.

D1–D3 należy wycenić oddzielnie w ofercie i rozliczeniu. Prace wspólne, w tym analizy, spotkania i wprowadzenie procedur, rozdziela się tylko raz. Jeden spójny dokument może pokrywać kilka wymagań, jeżeli zawiera indeks ich przyporządkowania.

3. Treść dokumentacji

SZBI obejmie co najmniej:

– zakres i role
– inwentaryzację aktywów, produktów, usług i procesów ICT z właścicielami
– klasyfikację i ochronę informacji oraz infrastruktury
– ocenę i postępowanie z ryzykiem
– zarządzanie tożsamością, uprawnieniami, uwierzytelnianiem i dostępem awaryjnym
– bezpieczne użytkowanie, pracę zdalną i urządzenia mobilne
– ochronę poczty i przed złośliwym oprogramowaniem
– rejestrowanie i analizę zdarzeń
– obsługę incydentów i wymaganych zgłoszeń
– kopie zapasowe i odtwarzanie
– zmiany, wersje, aktualizacje i podatności
– ochronę fizyczną, nośniki, transfer, kryptografię i bezpieczne usuwanie
– nadzór nad dostawcami i zdalnym serwisem IT/OT
– cyberhigienę i zasady szkoleń
– nadzór nad dokumentacją, przeglądy, planowanie audytów i sprawdzeń oraz działania korygujące.

Zakres dokumentów chmurowych, BYOD, rozwoju oprogramowania i innych rozwiązań szczególnych należy zweryfikować wobec faktycznych usług i dopuszczonych sposobów pracy. Każda procedura określi cel, zakres, właściciela i zastępcę, przesłanki uruchomienia, kolejne działania, wykonawców, terminy, eskalację, wymagane zapisy, powiązane dokumenty i kryteria zakończenia. Przygotowanie zasad, scenariuszy i formularzy nie obejmuje wykonania odrębnych testów, audytów, szkoleń ani ćwiczeń wyłączonych w części 7.

Dokumentacja ochrony danych osobowych musi pozostawać spójna z SZBI: PODO, rejestrami czynności, oceną ryzyka dla praw i wolności osób, upoważnieniami, obowiązkami informacyjnymi, realizacją praw osób, retencją, powierzeniem i obsługą naruszeń. Należy ustalić przesłanki DPIA, transferów poza EOG i stosowania zgód oraz opracować właściwe zasady lub uzasadnić ich niestosowanie. Wspólna obsługa zdarzeń musi rozróżniać ocenę, adresatów i terminy wynikające z KSC oraz RODO. Wykonawca przygotowuje lub aktualizuje dokumenty i formularze. Nie potwierdza fikcyjnego wykonania przyszłych czynności ani testów.

BIA wskaże krytyczne procesy, skutki przerw, minimalny poziom usług, zależności, personel i zasoby. Dla procesów i systemów należy uzgodnić maksymalny tolerowany okres zakłócenia MTPD, docelowy czas odtworzenia RTO i dopuszczalny okres utraty danych RPO, z określeniem początku i końca pomiaru. RTO z walidacją i osiągnięciem minimalnej usługi musi mieścić się w MTPD. Wartości wymagane, szacowane i potwierdzone wcześniejszymi próbami wykazuje się osobno.

BCP określi decyzję o uruchomieniu i zakończeniu trybu awaryjnego, eskalację, zastępstwa, alternatywną łączność, pracę ręczną lub zastępczą, zasoby, granice bezpiecznej kontynuacji, kontakty i komunikaty. BCP obejmie:

– brak energii lub dostępu do obiektu
– awarię IT i utratę danych
– awarię SCADA, telemetrii lub łączności
– cyberincydent albo niedostępność narzędzi ochrony
– zakłócenie dostaw lub jakości wody
– awarię kanalizacji i ryzyko przepełnienia
– niedostępność PSZOK lub BDO
– brak kluczowej osoby lub dostawcy.

Jeden wariant połączy awarię IT, łączności i absencję personelu.

DRP obejmie wszystkie krytyczne systemy w określonym zakresie albo uzasadnione grupy jednorodne. Instrukcje wskażą kolejność i zależności, kopie, konfiguracje, licencje, narzędzia, uprawnienia, kolejne kroki, oczekiwane wyniki, punkty kontrolne, warunki przerwania i wycofania, walidację danych oraz zgodę na wznowienie pracy. Uwzględnią ochronę przed ponowną kompromitacją i uzgodnienie zapisów z pracy zastępczej.

Plany będą dostępne uprawnionym osobom.

4. Sposób wykonania i wprowadzenie procedur

Wykonawca przeprowadzi przegląd materiałów, wywiady i uzgodnienia z właścicielami procesów. Cena obejmuje spotkanie otwierające i co najmniej dwa dni robocze wizyt w siedzibie PUK „PEKO”.

Spotkania służą ustaleniu braków dokumentacji, BIA, założeń odtwarzania i odpowiedzialności.

Wykonawca przygotuje wykaz dokumentów do zatwierdzenia.

Dokumentacja musi odzwierciedlać stan rzeczywisty. Przegląd i aktualizacja w tym zamówieniu są jednorazowymi pracami do odbioru, a nie stałym utrzymaniem systemów.

5. Wymagania wobec wykonawcy

Podmiot faktycznie opracowujący dokumenty musi wykazać co najmniej dwa lata doświadczenia w dokumentowaniu bezpieczeństwa informacji lub ciągłości działania oraz co najmniej dwa należycie zakończone opracowania lub aktualizacje SZBI w ostatnich trzech latach przed terminem ofert, w tym co najmniej jedno zadanie obejmujące BIA oraz BCP i DRP. Wymagania mogą być wykazane w tych samych umowach. Nie ogranicza się doświadczenia do wodociągów.

Osoba kierująca pracami ma co najmniej dwa lata praktyki i udział w co najmniej dwóch zakończonych pracach dokumentacyjnych SZBI w ostatnich pięciu latach. Posiada imienny certyfikat albo szkolenie zakończone egzaminem w obszarze ISO/IEC 27001 lub bezpieczeństwa informacji, np. Lead Implementer, Lead Auditor, CISM, CISSP, albo kwalifikację równoważną. Zespół łącznie wykaże co najmniej jedno zadanie BIA z BCP i DRP oraz jeden projekt dotyczący dokumentowania lub zabezpieczania IT/OT w ostatnich pięciu latach. Role może wykonywać jedna osoba spełniająca wszystkie warunki.

Równoważność oznacza porównywalny zakres wiedzy i niezależną weryfikację albo egzamin.

Wykonawca podaje osobę, wystawcę, datę, zakres i sposób potwierdzenia. Do oferty dołącza wykaz usług i osób oraz referencje lub inne dowody i kwalifikacje. Dopuszcza się doświadczenie u poprzednich pracodawców i podmioty udostępniające zasoby, które wykonają odpowiedni zakres. Samo ogólne oświadczenie albo data rejestracji firmy nie potwierdza doświadczenia.

Nie wymaga się uprawnienia audytora z art. 15 KSC ani statusu jednostki certyfikującej, ponieważ zamówienie dotyczy opracowania i wprowadzenia dokumentacji. Osoby tworzące dokumenty nie mogą następnie niezależnie audytować własnej pracy. Zastępstwa wymagają zachowania warunków i akceptacji PUK „PEKO”.

6. Wyniki i odbiór

Wykonawca przekaże dokumentację D1–D3 z analizami i rejestrem ryzyk oraz wykaz powiązań z konkretnymi wersjami i punktami istniejących polityk. Rozbieżności trzeba przedstawić PUK „PEKO” i uzyskać ich rozstrzygnięcie. Wymagane są polskie pliki DOCX lub ODT i przeszukiwalne PDF. Rejestry XLSX lub ODS, a schematy także w plikach źródłowych. Dokumenty mają identyfikator, wersję, datę, właściciela i historię zmian.

Wykonawca przekaże podpisane przez osobę kierującą pracami merytorycznymi zestawienie weryfikacji wszystkich 53 pozycji załącznika nr 2B oraz pozostałych wymagań OPZ. Dla każdej pozycji i wymagania wskaże dokument, identyfikator, wersję, datę i rozdział, wynik przeglądu, ustalony stan stosowania oraz wykonane zmiany. Wyniki: pozostawiono po weryfikacji, zaktualizowano, opracowano albo nie dotyczy z uzasadnieniem zaakceptowanym przez PUK „PEKO”. Zestawienie musi wskazywać rozstrzygnięcie każdej kolizji oraz miejsce pokrycia każdego właściwego wymagania. Jedna pozycja może odsyłać do kilku dokumentów i odwrotnie. Podpis potwierdza wykonanie przeglądu oraz kompletność i spójność końcowego pakietu w zakresie zamówienia. Nie zastępuje zatwierdzenia przez PUK „PEKO” ani niezależnego audytu. Wykonawca odpowiada również za wady treści pozostawionych po weryfikacji, które powinien był wykryć przy zachowaniu należytej staranności. Obejmuje je gwarancja na zasadach umowy.

Odbiór wymaga kompletnego, spójnego i dostosowanego do PUK „PEKO” pakietu, udokumentowanego wprowadzenia oraz rozpatrzenia uwag. Ogólne wzory z pustymi polami możliwymi do uzupełnienia nie stanowią wykonania. Ograniczenia i informacje niepotwierdzone wykazuje się jawnie. Odbiór nie jest pozytywną opinią audytową ani potwierdzeniem skuteczności technicznego odtwarzania. Warunkiem odbioru jest również kompletne zestawienie z poprzedniego akapitu oraz zgodność treści, wersji, formularzy i odwołań w całym przekazywanym pakiecie. Samo opisanie brakujących dokumentów nie zastępuje ich opracowania w zakresie zamówienia.

Wykonawca przekazuje pełny projekt D1–D3 do 04.12.2026 r. do godz. 12:00. PUK „PEKO” przekazuje uwagi do 07.12.2026 r. do godz. 15:00. Wykonawca przekazuje pełną, poprawioną dokumentację do 11.12.2026 r. do godz. 12:00. Do 11.12.2026 r. następują przyjęcie i przekazanie zasadniczych procedur prowadzącemu szkolenia oraz odbiór końcowy. Cena obejmuje jednorazową aktualizację do odbioru. Zasady poprawiania wad, w tym stwierdzonych po audycie, określa umowa.

7. Powiązanie ze szkoleniami i audytem

Zamówienie nie obejmuje niezależnych audytów SZBI, SZCD lub KRI/KSC, certyfikacji, utrzymania, zakupów lub konfiguracji infrastruktury, testów technicznych, prób odtworzenia, kampanii phishingowych ani ćwiczenia reagowania na incydent. Szkolenia ADM.014.2026.10.AS rozwijają i sprawdzają kompetencje na przyjętych procedurach, a audyt ADM.016.2026.10.AS niezależnie ocenia wyniki. Instruktażu przekazania dokumentacji nie wykazuje się jako tych samych godzin szkoleń. Wykonawca przekaże PUK „PEKO” materiały potrzebne do obu odrębnych usług.

Dokumentację techniczną powykonawczą, konfiguracje i instrukcje odtwarzania dostarczane w ramach wdrożenia serwerowni lub SCADA wykorzystuje się jako materiały wejściowe. Wykonawca D1–D3 sprawdza ich spójność z procesami PUK „PEKO”, uzupełnia powiązania, role i decyzje organizacyjne oraz włącza je do BCP/DRP. Nie zamawia się ponownie wykonania tych samych opracowań należnych od integratora. Braki techniczne zgłasza się PUK „PEKO” z określeniem ich wpływu na możliwość użycia planów.

8. Podstawy opracowania poufność i prawa

Dokumenty uwzględnią aktualne wymagania ustawy o krajowym systemie cyberbezpieczeństwa (KSC), KRI w zakresie stosowania do PUK „PEKO”, RODO, ustawy o zarządzaniu kryzysowym w zakresie właściwym dla PUK „PEKO” i przepisów sektorowych oraz pomocniczo ISO/IEC 27001:2022 i ISO 22301:2019 wraz

z właściwymi zmianami albo podejście równoważne w zakresie ryzyka, BIA, odpowiedzialności, ciągłości i nadzoru nad dokumentacją. Wykonawca zweryfikuje podstawy samooceny PUK „PEKO” jako podmiotu ważnego, status podmiotu publicznego na gruncie KSC i właściwy zakres obowiązków, w tym dokumentowania i zgłoszeń. Obowiązki dotyczące infrastruktury krytycznej lub podmiotu krytycznego ujmuje się tylko po potwierdzeniu przesłanek ich stosowania. Samo świadczenie usług wodociągowych lub kanalizacyjnych nie zastępuje tego ustalenia. Wynik i podstawy odnotowuje się w karcie kwalifikacji oraz rejestrze wymagań. Ustalenie tych wymagań dla opracowania dokumentów nie jest niezależnym audytem zgodności.

Dane są poufne. Dostęp jest imienny i ograniczony, wymiana i przechowywanie szyfrowane, a dane i kopie pozostają w UE. Nie wolno używać ich do własnego marketingu, profilowania ani trenowania AI. Zdalny dostęp z państwa trzeciego wymaga uprzedniej pisemnej zgody PUK „PEKO” i spełnienia RODO. Potrzebne powierzenie i zgody na podwykonawców ustala się przed dostępem. Naruszenie danych zgłasza się niezwłocznie, najpóźniej w 24 godziny. Krytyczne zagrożenie bezpieczeństwa niezwłocznie, nie później niż w 4 godziny.

Cena obejmuje wszystkie prace, dojazdy, materiały, poprawki i prawa do używania, kopiowania, aktualizowania i przekazywania dokumentacji uprawnionym osobom, audytorom, organom i kolejnym usługodawcom. Wykonawca udzieli 24 miesięcy gwarancji na wady własnych opracowań, zgodnie z umową. Gwarancja nie obejmuje stałego utrzymania ani aktualizacji wyłącznie z powodu późniejszych zmian prawa, systemów lub organizacji.