Załącznik nr 4 do zaproszenia do złożenia oferty

/Projekt/

Umowa na przeprowadzenie audytu cyberbezpieczeństwa

Numer postępowania ADM.016.2026.10.AS

Umowa nr ..... zawarta w Kosakowie dnia ..... pomiędzy: Przedsiębiorstwem Usług Komunalnych „PEKO” sp. z o.o. w Kosakowie, ul. Chrzanowskiego 44, 81-198 Kosakowo, NIP 9581154984, REGON 191416896, KRS 0000038875, reprezentowanym przez ....., dalej „PEKO” lub „Zamawiający”, a ....., NIP ....., reprezentowanym przez ....., dalej „Wykonawca”.

§ 1 Przedmiot umowy

1. Wykonawca przeprowadzi niezależny audyt oraz testy A1–A5 i T1–T3 według OPZ i skali środowiska, stanowiących załączniki nr 2 i 2A do zaproszenia. Zamówienie jest częścią projektu „Kompleksowa rozbudowa i modernizacja rozwiązań z zakresu cyberbezpieczeństwa w PUK PEKO”, program „Cyberbezpieczne Wodociągi”, inwestycja C3.1.1 KPO.
2. Nieodłączną część umowy stanowi OPZ, załącznik nr 2a oraz oferta.
3. Usługa nie obejmuje wdrażania zaleceń, usuwania podatności, tworzenia procedur, szkoleń, phishingu ani certyfikacji. Audytor ocenia rzeczywiście istniejący stan i dowody; nie gwarantuje pozytywnego wyniku ani rozliczenia grantu.
4. T1–T3 są niezależnymi testami bezpieczeństwa audytora po wdrożeniu. Testy funkcjonalne, odbiorowe, pierwsze skanowanie i usuwanie wad należą do wykonawców wdrożeń; ich protokoły są materiałem wejściowym. Audytor określi własne cele, metody i wyniki T1–T3 oraz odróżni je od dostarczonych protokołów. Nie rozlicza jako własnej usługi czynności wykonanych przez integratora. Obserwacja próby odtworzenia może odbyć się przy teście integratora; audytor rozlicza wyłącznie własną obserwację i ocenę.

§ 2 Organizacja i terminy

Etap	Termin i odpowiedzialność
Przygotowanie	Wykonawca do 3 dni roboczych od umowy: plan, dobór próby i obiektów, lista materiałów, terminy wizyt i zasady bezpiecznych testów do akceptacji PUK „PEKO” Sp. z o.o.. Przegląd dostępnych dokumentów i istniejącego środowiska rozpoczyna się bez oczekiwania na zakończenie całej modernizacji.
Dokumentacja	PUK „PEKO” Sp. z o.o. przekazuje przyjęte procedury sukcesywnie, a końcową dokumentację SZBI, SZCD, BIA, BCP i DRP wraz z dowodami przyjęcia do 11.12.2026. Audytor ocenia ostateczne wersje i dowody stosowania.
Gotowość środowiska	PUK „PEKO” Sp. z o.o. do 14.12.2026 zapewnia uruchomione rozwiązania IT/OT, separację IT/OT, dostępy, dokumentację powykonawczą oraz odseparowane środowisko testowe SCADA i operatora próby odtworzenia, zgodnie z 2A.
Dowody szkoleń	PUK „PEKO” Sp. z o.o. udostępnia dostępne dowody odrębnych szkoleń, kampanii i ćwiczenia sukcesywnie, do 16.12.2026; uzupełnienia przekazuje niezwłocznie do zakończenia badania. Audytor uwzględnia daty i ograniczenia dowodów.

Etap	Termin i odpowiedzialność
Zasadnicze badania	Wykonawca do 18.12.2026 wykonuje zasadnicze badania i testy oraz przekazuje raporty, rejestry, macierze i dowody do uwag PUK „PEKO” Sp. z o.o.. Ustalenia krytyczne zgłasza od razu zgodnie z OPZ.
Uwagi i poprawki	PUK „PEKO” Sp. z o.o. zgłasza uwagi do raportów do 21.12.2026. PUK „PEKO” Sp. z o.o. lub integratorzy wykonują poprawki zabezpieczeń do 22.12.2026 i przekazują audytorowi ich wykaz oraz dowody gotowości do ponownej weryfikacji.
Raport końcowy	Wykonawca przeprowadza jedną ponowną weryfikację zgłoszonych poprawek i przekazuje podpisany raport końcowy do 28.12.2026 godz. 12:00. Niesprawdzone lub niewykonane działania pozostają otwarte.
Odbiór i rozliczenie	PUK „PEKO” Sp. z o.o. zgłasza uwagi do kompletności i rzetelności raportu końcowego do 29.12.2026 godz. 10:00; Wykonawca usuwa własne wady raportu do 29.12.2026 godz. 18:00. Prezentacja i odbiór do 30.12.2026 godz. 12:00, prawidłowa faktura tego dnia, płatność do 31.12.2026 według § 5.

1. Dni robocze to poniedziałek–piątek z wyłączeniem dni ustawowo wolnych w Polsce. Wykonawca realizuje co najmniej dwa dni czynności na miejscu, spotkanie otwierające i końcowe. Szczegółowe terminy uzgadniają koordynatorzy w granicach powyższego harmonogramu.
2. PUK PEKO Sp.z o.o. zapewnia dokumenty, dostępy, zgody i upoważnioną obsługę oraz z integratorem odseparowane środowisko testowe SCADA na infrastrukturze wirtualnej projektu, licencje, kopię i operatora odtworzenia, zgodnie z 2A. PUK PEKO Sp.z o.o. organizuje i pokrywa udział integratora; nie obciąża tym wynagrodzenia audytora. Wykonawca zapewnia zespół, dojazdy i własne narzędzia badania. Cena audytora nie obejmuje budowy pełnej repliki SCADA. Odtworzenie wykonuje się z rzeczywistej kopii w izolacji, bez nadpisania produkcji i bez sterowania urządzeniami; audytor obserwuje, mierzy i weryfikuje wynik.
3. Cena obejmuje jedną ponowną bezpieczną weryfikację pierwotnych ustaleń krytycznych i wysokich, jeżeli ich przyczyny zostaną usunięte do 22.12.2026. Niewykonanych lub niesprawdzonych działań nie wykazuje się jako zakończonych. Nie oznacza to obowiązku wdrożenia poprawek przez audytora.
4. Strony niezwłocznie zgłaszają przeszkody i uzgadniają działania naprawcze. Brak gotowości nie uprawnia do potwierdzenia niewykonanej usługi ani automatycznego przesunięcia dat. Wykonawca nie odpowiada za zwłokę spowodowaną wyłącznie udokumentowanym brakiem współdziałania PUK PEKO Sp.z o.o. Zmiana dat granicznych wymaga zasad z § 9 i oceny skutków dla projektu.
5. Koordynator PEKO: ....., e-mail .....; koordynator Wykonawcy: ....., e-mail ..... . Koordynatorzy nie mogą zmieniać ceny, zakresu ani dat granicznych bez upoważnienia.

§ 3 Personel i bezpieczeństwo

1. Wykonawca zapewnia, co najmniej dwuosobowy zespół o wymaganych rolach, doświadczeniu, uprawnieniach i niezależności. Zastępstwo lub podwykonawca wymaga uprzedniej pisemnej akceptacji PUK „PEKO” Sp. z o.o. i dowodów spełnienia warunków. Wykonawca odpowiada za ich działania jak za własne.
2. Prace wymagają zatwierdzonych zasad testów obejmujących zasoby, metody, upoważnienia, okna, kopie, warunki przerwania i kontakt alarmowy. Wymagane zgody dostawców uzyskuje się przed pracami. Obowiązują zakazy i ograniczenia z części 4a OPZ, dziennik działań, możliwość natychmiastowego zatrzymania i ochrona ciągłości usług. Samo podpisanie umowy nie upoważnia do aktywnego skanowania sterowników.

3. Podatność krytyczną lub podejrzenie trwającego naruszenia Wykonawca zgłasza niezwłocznie, nie później niż 4 godziny od wykrycia, telefonicznie oraz bezpiecznym kanałem pisemnym. Kontakty alarmowe strony ustalą przed dostępem do systemów.

§ 4 Raporty i odbiór

1. Wykonawca przekazuje po polsku plan, raporty organizacyjne i techniczne, raport końcowy, macierz wymagań, rejestr niezgodności i podatności, ocenę ryzyka, plan działań, dowody testów i próby odtworzenia. Jedno opracowanie może zawierać wyraźne części A1–A5 i T1–T3. Wykonawca prezentuje wyniki i udziela wyjaśnień PUK „PEKO” Sp. z o.o.
2. Każde ustalenie wskazuje kryterium, dowód, wpływ i zalecenie. Raport rozróżnia obowiązki prawne i dobre praktyki, stan rzeczywisty i deklarowany, ograniczenia oraz elementy niewykonane. Dokumentuje zakres próby i rzeczywiste metody.
3. Raporty przekazuje się jako DOCX lub ODT i podpisany, przeszukiwalny PDF, a rejestry i macierze jako XLSX lub ODS. Dane wrażliwe należy oddzielić do chronionego załącznika. Podpisany raport zawiera dane i kwalifikacje audytorów, zakres i daty badania oraz wnioski i dowody wymagane dla właściwego rodzaju audytu.
4. Odbiór następuje na podstawie kompletnej, rzetelnie wykonanej usługi i protokołu według załącznika nr 7 do zaproszenia. Samo przekazanie plików lub milczenie PUK „PEKO” Sp. z o.o. nie oznacza odbioru. Spółka zgłasza konkretne braki w terminie 3 dni; Wykonawca poprawia własne błędy i uzupełnia wymagane dowody w cenie, w terminach § 2. Raport negatywny lub wykryte podatności nie stanowią same w sobie wady usługi.
5. Ustalenia dotyczące bezpieczeństwa PUK „PEKO” Sp. z o.o. nie muszą zostać usunięte, aby odebrać rzetelny audyt. Odbiór nie zależy od pozytywnej oceny organizacji. Istotnego niewykonania testów lub braków raportu nie zastępuje oświadczenie. Sporny zakres i przyczyny strony opisują odrębnie; brak finansowania grantowego nie uzasadnia potwierdzenia niewykonanych czynności.

§ 5 Wynagrodzenie i zapłata

1. Łączne wynagrodzenie ryczałtowe wynosi ..... zł netto, VAT ..... zł, razem ..... zł brutto. Podział na A1–A5 i T1–T3 wynika z formularza cenowego. Nie przewiduje się opcji. Cena obejmuje wszystkie wymagane czynności i koszty; wspólne prace nie są naliczane ponownie.
2. Wykonawca wystawi i doręczy prawidłową fakturę niezwłocznie po końcowym odbiorze, najpóźniej 30.12.2026. Faktura lub zestawienie do niej rozdziela osiem pozycji, netto, VAT i brutto oraz daty świadczenia i dowód odbioru. Faktury wystawia się i doręcza zgodnie z przepisami, w tym KseF.
3. Zapłata nastąpi przelewem w ciągu 7 dni kalendarzowych od otrzymania prawidłowej faktury po odbiorze, jednak nie później niż 31.12.2026, jeżeli prawidłowa faktura wpłynie do 30.12.2026. Wykonawca nie wystawia faktury za niezakończoną usługę jako wykonaną. Późniejszy wpływ wymaga zapłaty w terminie 7 dni i odrębnej oceny finansowania; nie zmienia dat kwalifikowalności. Zapłata nie zależy od otrzymania grantu. Nie przewiduje się zaliczki.

§ 6 Poufność i dane

1. Wykonawca zachowuje poufność danych, konfiguracji, wyników i informacji o zabezpieczeniach także po umowie. Udostępnia je wyłącznie upoważnionym, zobowiązanym do poufności osobom, w niezbędnym zakresie. Bez uprzedniej zgody PUK „PEKO” Sp. z o.o. nie publikuje nazwy ani materiałów projektu jako referencji lub studium przypadku.
2. Obowiązują szyfrowane kanały i przechowywanie, oddzielne przekazywanie haseł, dane i kopie w UE oraz zakaz wykorzystania do własnego marketingu, profilowania i trenowania AI. Zdalny dostęp z państwa trzeciego wymaga uprzedniej pisemnej zgody PUK „PEKO” Sp. z o.o. i spełnienia wymagań usawy o cyberbezpieczeństwie i ochrony danych bez naruszenia lokalizacji danych w UE. Powierzenie i podwykonawcy wymagają uzgodnień określonych w OPZ.

3. Przed dostępem do danych Zamawiającego strony podpiszą umowę zgodną z załącznikiem nr 6. Naruszenie danych zgłasza się niezwłocznie, najpóźniej w 24 godziny od stwierdzenia tego faktu na odo@pukpeko.pl oraz koordynatorowi; dla zagrożeń z § 3 ust. 3 obowiązuje termin 4 godzin.
4. Po zakończeniu Wykonawca rozliczy i zamknie dostępy, zwróci materiały oraz potwierdzi usunięcie kopii na zasadach powierzenia, jeśli ma zastosowanie. Pozostałe poufne kopie robocze usuwa w ciągu 30 dni, a odizolowane kopie bezpieczeństwa w 90 dni. Obowiązek zachowania dokumentacji z mocy prawa wymaga wskazania podstawy, zakresu i czasu oraz dalszej ochrony, bez własnego wykorzystania.

§ 7 Korzystanie z wyników

1. W cenie, z chwilą przekazania wyników, Wykonawca udziela PUK „PEKO” Sp. z o.o. licencji na czas nieoznaczony i bez ograniczeń terytorialnych do przechowywania i utrwalania raportów, macierzy i rejestrów w pamięci urządzeń, zwielokrotniania drukiem i cyfrowo, wewnętrznego udostępniania, przekazywania organom, instytucjom projektu, kontrolującym, audytorom i wykonawcom działań naprawczych oraz modyfikacji i aktualizacji do celów własnych PUK „PEKO” Sp. z o.o.
2. Wykonawca zapewnia prawa do udzielonej licencji i zgodę na opracowania w powyższym zakresie. Uprawnienia obejmują dowody i dokumentację niezbędne do użycia wyników. Licencje narzędzi osób trzecich nie mogą ograniczać korzystania z raportów. Umowa nie przenosi własności narzędzi audytora ani praw osób trzecich poza zakresem niezbędnym do użycia wyników.

§ 8 Odpowiedzialność i rozwiązanie umowy

1. Za zwłokę w przekazaniu kompletnych wyników lub usunięciu wad raportu Wykonawca zapłaci 0,2% wynagrodzenia brutto za każdy rozpoczęty dzień. Nie nalicza się dwóch kar za ten sam okres i to samo uchybienie. Za zawinione naruszenie poufności, niezależności lub zatwierdzonych zasad bezpiecznych testów kara wynosi 5% wynagrodzenia brutto za zdarzenie. Za odstąpienie lub rozwiązanie z przyczyn zawinionych przez Wykonawcę — 10%. Łączny limit kar to 20% wynagrodzenia brutto.
2. PUK „PEKO” Sp. z o.o. może dochodzić odszkodowania przewyższającego kary na zasadach ogólnych. Potrącenie wymaga wymagalności i oświadczenia. Wykonawca ma prawo do ustawowych odsetek za opóźnienie zapłaty. Kary nie obejmują okoliczności, za które Wykonawca nie ponosi odpowiedzialności.
3. Przy istotnym naruszeniu PUK „PEKO” Sp. z o.o. może rozwiązać umowę w niezrealizowanej części po pisemnym wezwaniu i bezskutecznym upływie 3 dni roboczych na usunięcie naruszenia. Przy bezpośrednim zagrożeniu ciągłości usług, ciężkim naruszeniu poufności lub braku niezależności PUK „PEKO” Sp. z o.o. może natychmiast wstrzymać dostęp i rozwiązać umowę bez dodatkowego terminu. Rozwiązanie następuje przez pisemne oświadczenie, ze wskazaniem przyczyn i rozliczeniem rzeczywiście wykonanego, przydatnego i przekazanego zakresu; nie potwierdza kwalifikowalności niewykonanej części.

§ 9 Zmiany i postanowienia końcowe

1. Zmiany wymagają formy pisemnej albo elektronicznej z podpisami kwalifikowanymi oraz zgodności z właściwymi zasadami konkurencyjności. Dopuszcza się: zmianę personelu na spełniający nie mniejsze wymagania; zmianę terminów cząstkowych z powodu udokumentowanych ograniczeń bezpieczeństwa, siły wyższej lub opóźnionej gotowości PUK „PEKO” Sp. z o.o.; zmianę sposobu fakturowania wymaganą prawem; zmianę VAT wynikającą z przepisów przy zachowaniu netto dla niewykonanej części.
2. Zmiana organizacji nie może usuwać obowiązkowych obszarów, obniżać niezależności, zastępować testów pozornym wykonaniem ani podwyższać wynagrodzenia bez dopuszczalnej podstawy. Zmiana daty końcowej wymaga odrębnej podstawy zgodnej z regułami konkurencyjności i uprzedniej oceny skutków dla grantu; sama ta klauzula nie przedłuża terminu projektu ani finansowania. Inne zmiany wyłącznie w granicach właściwych reguł, z pisemnym uzasadnieniem.

3. Nie ustanawia się odrębnej gwarancji ani usługi utrzymania systemów. Obowiązek poprawienia wad własnej dokumentacji oraz odpowiedzialność ustawowa pozostają w mocy. Spory strony starają się rozwiązać polubownie, a następnie przed sądem właściwym według przepisów ogólnych. W sprawach nieuregulowanych stosuje się prawo polskie, w szczególności Kodeks cywilny i RODO.

Zamawiający:	Wykonawca:
.....…….....	.....……..