# ZAPYTANIE OFERTOWE

## Dla zamówień o wartości do 170.000,00 zł netto

1. **Nazwa i adres ZAMAWIAJĄCEGO:**
   Przedsiębiorstwo Wodno –Kanalizacyjne Sp. z o.o. w Czarnem ,
   77-330 Czarne
   Al. Zwycięzców 1c

2. **Przedmiot zamówienia:**

   **Opracowanie, wdrożenie oraz wsparcie we wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnego z wymaganiami ustawy o krajowym systemie cyberbezpieczeństwa (KSC), Dyrektywy NIS2, Rozporządzenia KRI oraz normy ISO/IEC 27001:2022.**
   Zakres usługi powinien obejmować:

   **Projektowanie systemu zarządzania bezpieczeństwem informacji poprzez następujące procedury i zagadnienia:**

   - Opracowanie procedury identyfikacji wymagań dla Systemu Zarządzania Bezpieczeństwem Informacji
     1. Identyfikacja zainteresowanych stron
     2. Inwentaryzacja wymagań prawnych, branżowych, umownych i innych wymagań związanych z bezpieczeństwem informacji
     3. Określenie ról i osób odpowiedzialnych za spełnienie w/w wymagań
   - Opracowanie Polityki Bezpieczeństwa Informacji
     1. Określenie Zakresu Systemu Zarządzania Bezpieczeństwem Informacji
     2. Opis celów zarządzania bezpieczeństwem informacji
     3. Przypisanie odpowiedzialności i ról w zakresie utrzymywania SZBI
   - Przygotowanie Metodyki Szacowania i Postępowania z Ryzykiem
     1. Opis metodyki
     2. Określenie sposobu wyliczenia ryzyka
     3. Opis metod akceptacji poszczególnych wartości ryzyka

4. Stworzenie wzoru tabeli szacowania ryzyka, tabeli postępowania z ryzykiem, tabele zawierają przykładowe aktywa, zagrożenia i podatności
5. Wzór raportu z dokonanego szacowania ryzyka
6. Przeprowadzenie analizy stanu obecnego (Gap Analysis), obejmującej ocenę zgodności organizacji z wymaganiami KSC, NIS2, KRI oraz ISO/IEC 27001 wraz z opracowaniem planu działań naprawczych.

- Opracowanie Deklaracji Stosowania (Statement of Applicability – SoA), zawierającej opis zastosowanych zabezpieczeń oraz uzasadnienie ich wdrożenia lub niewdrożenia zgodnie z ISO/IEC 27001:2022.
- Opracowanie rejestrów SZBI obejmujących:
    1. Rejestru aktywów
    2. Rejestru ryzyk
    3. Rejestru incydentów
    4. Rejestru wyjątków bezpieczeństwa
    5. Rejestru dostawców
    6. Planu doskonalenia SZBI
- Opracowanie Planu postępowania z ryzykiem, zawierający opis działania z poszczególnym ryzykiem wraz z szczegółowymi informacjami na temat działań, które mają zostać podjęte
- Przygotowanie procedury audytu wewnętrznego
    1. Opis opracowywania planów audytu
    2. Opis metod przeprowadzania audytów oraz opracowywania raportów
    3. Dodatkowo dołączony wzór rocznego programu audytu wewnętrznego
- Przygotowanie wzoru protokołu z przeglądu SZBI dokonywanego przez kierownictwo
- Przygotowanie procedury działań naprawczych i działań korygujących w ramach wykrytych niezgodności
- Przygotowanie Procedur Operacyjnych dla zarządzania systemami informatycznymi zawierające:
    1. Polityki haseł

2. Polityki rozwoju systemów informatycznych, zawierające wzór wykazu systemów
3. Procedury dot. kopii zapasowych, wraz z wzorcem zasad ich tworzenia i przechowywania
4. Procedury dot. środowiska testowego i eksploatacji systemów wraz z dokumentowaniem zmian wraz z przygotowanymi wzorcami dokumentacji dotyczącej infrastruktury teleinformatycznej
5. Procedury niszczenia danych i wycofania systemów z eksploatacji
6. Procedury zabezpieczenia systemów
7. Procedury dot. posługiwania się nośnikami wymiennymi
8. Procedury dotyczące pracy w sieci Internet
9. Procedury dotyczące serwisu i przeglądu systemów informatycznych
10. Procedury dotyczące monitoringu infrastruktury i raportowania funkcjonowania środowiska teleinformatycznego
11. Procedura zarządzania podatnościami
12. Procedura zarządzania aktualizacjami bezpieczeństwa
13. Procedura zarządzania tożsamością i dostępem
14. Procedura zarządzania dostawcami (Supply Chain Security)
15. Procedura reagowania na incydenty cyberbezpieczeństwa
16. Procedura zgłaszania incydentów do właściwego CSIRT
17. Procedura zarządzania aktywami
18. Procedura szyfrowania danych
19. Procedura monitorowania bezpieczeństwa
20. Procedura zarządzania logami
21. Plan Ciągłości Działania (BCP)
22. Plan Odtwarzania po Awarii (DRP)

- Opracowanie rekomendacji technicznych obejmujących:
  1. segmentację sieci,
  2. MFA,
  3. zarządzanie podatnościami,
  4. SIEM,
  5. EDR/XDR,

6. backup,
7. monitoring,
8. logowanie,
9. szyfrowanie,
10. bezpieczeństwo dostawców,
11. ochronę środowisk OT

**Szkolenie z zakresu cyberbezpieczeństwa dla pracowników powinno obejmować poniższe zagadnienia:**

**1. Ataki komputerowe**

✓ Administrator danych osobowych

✓ Incydenty w skali roku

✓ Kary na Administratorów

✓ Cel ataków

✓ Motywacje włamywaczy

✓ Kim może być atakujący?

✓ Powody ataków

✓ Cel atakujących

✓ Ochrona przed atakami

✓ Wymagania prawne

**2. Czynnik ludzki – zagrożenia socjotechniczne**

✓ Czym jest socjotechnika

✓ Przykłady zagrożeń socjotechnicznych wraz z omówieniem – phishing

✓ Przykłady zagrożeń socjotechnicznych pisma

✓ Zagrożenia, do czego mogą prowadzić?

✓ Zasady wykonywania przelewów – bankowość elektroniczna

✓ Zagrożenia, płatności kartami bankowymi

✓ Środki bezpieczeństwa, przykłady – warsztat

✓ Środki ostrożności – socjotechnika

**3. Zasady bezpieczeństwa – jak chronić się przed zagrożeniami**

✓ Czyste biurko i ekran

✓ Hasła, złożoność i stosowanie

✓ Bezpieczne surfowanie w sieci Internet

✓ Korzystanie z sieci komputerowych

✓ Przykłady narzędzi

✓ Reagowanie na incydenty i włamania.

3. **Szkolenie powinno obejmować również:**

✓ obowiązki wynikające z ustawy KSC,

✓ obowiązki kierownictwa wynikające z NIS2,

✓ bezpieczeństwo pracy zdalnej,

✓ ochronę przed ransomware,

**Audyt wstępny zgodny z wymaganiami ustawy o krajowym systemie cyberbezpieczeństwa, Dyrektywy NIS2, Rozporządzenia KRI oraz normy ISO/IEC 27001:2022.**

**Zakres audytu :**

- ✓ Dokumentacja z zakresu bezpieczeństwa informacji
- ✓ Analiza zagrożeń związanych z przetwarzaniem informacji
- ✓ Inwentaryzacja sprzętu i oprogramowania informatycznego
- ✓ Zarządzanie uprawnieniami do pracy w systemach informatycznych
- ✓ Szkolenia pracowników zaangażowanych w proces przetwarzania informacji
- ✓ Praca na odległość i mobilne przetwarzanie danych
- ✓ Serwis sprzętu informatycznego i oprogramowania
- ✓ Procedury zgłaszania incydentów naruszeń bezpieczeństwa informacji

- ✓ Audyt wewnętrzny w zakresu bezpieczeństwa informacji
- ✓ Sprawdzenie procedur dotyczących kopii
- ✓ Wykonywanie ww. procedur
- ✓ Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych
- ✓ Zabezpieczenia techniczno-organizacyjne dostępu do informacji
- ✓ Zabezpieczenia techniczno-organizacyjne systemów informatycznych
- ✓ Rozliczalność działań w systemach informatycznych
- ✓ Ocena zgodności organizacji z wymaganiami ustawy o krajowym systemie cyberbezpieczeństwa (KSC) oraz Dyrektywy NIS2.
- ✓ Ocena skuteczności procesu zarządzania ryzykiem w obszarze cyberbezpieczeństwa.
- ✓ Ocena procesu zarządzania podatnościami, aktualizacjami bezpieczeństwa oraz ich dokumentowania.
- ✓ Ocena procesu zarządzania incydentami cyberbezpieczeństwa, w tym gotowości do zgłaszania incydentów właściwemu CSIRT.
- ✓ Ocena bezpieczeństwa łańcucha dostaw oraz sposobu zarządzania ryzykiem związanym z dostawcami usług i produktów ICT.
- ✓ Ocena skuteczności monitorowania bezpieczeństwa, rejestrowania zdarzeń oraz analizy logów.

**Audyt końcowy zgodny z wymaganiami ustawy o krajowym systemie cyberbezpieczeństwa, Dyrektywy NIS2, Rozporządzenia KRI oraz normy ISO/IEC 27001:2022.**

**Zakres audytu :**

- ✓ Dokumentacja z zakresu bezpieczeństwa informacji
- ✓ Analiza zagrożeń związanych z przetwarzaniem informacji
- ✓ Inwentaryzacja sprzętu i oprogramowania informatycznego
- ✓ Zarządzanie uprawnieniami do pracy w systemach informatycznych
- ✓ Szkolenia pracowników zaangażowanych w proces przetwarzania informacji
- ✓ Praca na odległość i mobilne przetwarzanie danych
- ✓ Serwis sprzętu informatycznego i oprogramowania
- ✓ Procedury zgłaszania incydentów naruszeń bezpieczeństwa informacji

- ✓ Audyt wewnętrzny w zakresu bezpieczeństwa informacji
- ✓ Sprawdzenie procedur dotyczących kopii
- ✓ Wykonywanie ww. procedur
- ✓ Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych
- ✓ Zabezpieczenia techniczno-organizacyjne dostępu do informacji
- ✓ Zabezpieczenia techniczno-organizacyjne systemów informatycznych
- ✓ Rozliczalność działań w systemach informatycznych
- ✓ Ocena zgodności organizacji z wymaganiami ustawy o krajowym systemie cyberbezpieczeństwa (KSC) oraz Dyrektywy NIS2.
- ✓ Ocena skuteczności procesu zarządzania ryzykiem w obszarze cyberbezpieczeństwa.
- ✓ Ocena procesu zarządzania podatnościami, aktualizacjami bezpieczeństwa oraz ich dokumentowania.
- ✓ Ocena procesu zarządzania incydentami cyberbezpieczeństwa, w tym gotowości do zgłaszania incydentów właściwemu CSIRT.
- ✓ Ocena bezpieczeństwa łańcucha dostaw oraz sposobu zarządzania ryzykiem związanym z dostawcami usług i produktów ICT.
- ✓ Ocena skuteczności monitorowania bezpieczeństwa, rejestrowania zdarzeń oraz analizy logów.
- ✓ Audyt końcowy powinien obejmować również weryfikację skuteczności wdrożonych działań naprawczych oraz ocenę stopnia osiągnięcia zgodności z wymaganiami KSC, Dyrektywy NIS2, Rozporządzenia KRI i normy ISO/IEC 27001:2022.
- ✓ Audyt końcowy powinien zostać wykonany w terminie 30 dni od dnia otrzymania od Zamawiającego informacji o wdrożeniu wszystkich rozwiązań IT , jednak nie później niż do dnia 18 grudnia 2026 .

4. **Warunki udziału w postępowaniu:**
   - Posiadanie potencjału technicznego i osobowego niezbędnego do wykonania zamówienia. Wykonawca złoży w tym zakresie oświadczenie będące załącznikiem do oferty.
   - Posiadanie doświadczenia w wykonywaniu audytów wynikających z Rozporządzenia 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)

- Wykonawca złoży w tym zakresie oświadczenie będące załącznikiem do oferty.
- Wykonawca musi posiadać minimum 3 letnie doświadczenie w wykonywaniu Audytów Bezpieczeństwa.
- Wszystkie wyżej wymienione usługi muszą zostać przeprowadzone w siedzibie Zamawiającego.
- Dodatkowe wymagania:
- • Czas trwania: dostosowany do tematyki. Wykonawca zapewni możliwość realizacji szkolenia w dzień roboczy od poniedziałku do piątku w godzinach od 8:00 do 14:00, po wcześniejszym uzgodnieniu dokładnego terminu z Zamawiającym,
- • Zamawiający udostępni Wykonawcy miejsce na czas przeprowadzenia szkolenia,
- • Wykonawca zapewni odpowiedni sprzęt i oprogramowanie na potrzeby realizacji szkolenia, • Wykonawca zobowiązany będzie do przygotowania i przekazania uczestnikom materiałów szkoleniowych w języku polskim, w formie elektronicznej (plik w formacie PDF przesłany na wskazany przez Zamawiającego adres e-mail) i papierowej (w ilości odpowiadającej liczbie uczestników). Zamawiający przekaże Wykonawcy najpóźniej na 2 dni przed planowanym szkoleniem listę uczestników,
- • Wykonawca zobowiązany będzie wydać uczestnikom szkolenia, którzy ukończyli szkolenie, imienne zaświadczenie o ukończeniu w szkolenia,
- • Po zakończeniu szkolenia Wykonawca przekaże Zamawiającemu jeden komplet materiałów przekazanych uczestnikom oraz kompletną treść prezentacji multimedialnej wykorzystywanej przez prowadzącego w trakcie szkolenia (1 egzemplarz w wersji papierowej i 1 egzemplarz w wersji elektronicznej w formacie PDF i edytowalnym, na zewnętrznym nośniku danych),
- • Wszelkie dokumenty wytworzone i przekazane przez Wykonawcę w ramach realizacji zamówienia, w tym materiały szkoleniowe i zaświadczenia muszą uwzględniać wymogi Konkursu grantowego „Cyberbezpieczne Wodociągi", spełniać standardy dostępności oraz być prawidłowo oznakowane w zakresie informacji i promocji, z uwzględnieniem logotypów obowiązujących dla w/w Konkursu,
- • Wszelkie czynności i prace winny być prowadzone z zachowaniem zasady poufności i zgodności z RODO.

**5. Kryteria oceny oferty:**

- cena 100%

6. **Termin realizacji zamówienia:**
   1 m-c od dnia zawarcia umowy

7. **Sposób przygotowania oferty:**
   - elektronicznie na adres pwkczarne@wp.pl
   - wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty

8. **Termin składania ofert:**
   14 dni od ukazania się oferty

9. **Zamawiający nie dopuszcza składania ofert wariantowych.**
10. **Osoby uprawione do kontaktów z wykonawcami:**
    Edward Jankowski, Prezes Zarządu PW-K Czarne Sp. z o.o.
11. **Klauzula informacyjna z art. 13 RODO**

**OŚWIADCZENIE O WYRAŻENIU ZGODY**

Wyrażam zgodę na przetwarzanie moich danych osobowych w zakresie zgodnym z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), publ. Dz. Urz. UE L Nr 119, s. 1 w celu zawarcia i wykonania umowy-zlecenia.

**KLAUZULA INFORMACYJNA**

1. Administratorem Pani/Pana danych osobowych Przedsiębiorstwo Wodno-Kanalizacyjne Spółka z o.o. z siedzibą w Czarnem, 77-330 Czarne, ul. Al. Zwycięzców 1c, ,59 833 36 72
2. W sprawach z zakresu ochrony danych osobowych mogą Państwo kontaktować się z Administratorem Ochrony Danych pod adresem e-mail: pwkczarne@wp.pl
3. Dane osobowe będą przetwarzane w celu zawarcia i wykonania umowy-zlecenia.
4. Dane osobowe będą przetwarzane do czasu cofnięcia zgody na przetwarzanie danych osobowych.
5. Podstawą prawną przetwarzania danych jest art. 6 ust. 1 lit. a) ww. Rozporządzenia.
6. Odbiorcami Pani/Pana danych będą podmioty, które na podstawie zawartych umów przetwarzają dane osobowe w imieniu Administratora.
7. Osoba, której dane dotyczą ma prawo do:

- żądania dostępu do danych osobowych oraz ich sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych.
- cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.
- wniesienia skargi do organu nadzorczego w przypadku gdy przetwarzanie danych odbywa się z naruszeniem przepisów powyższego rozporządzenia tj.

Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

Podanie danych osobowych jest dobrowolne, przy czym konsekwencją niepodania danych osobowych jest odmowa zawarcia i wykonania umowy-zlecenia.

Ponadto informujemy, iż w związku z przetwarzaniem Pani/Pana danych osobowych nie podlega Pan/Pani decyzjom, które się opierają wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, o czym stanowi art. 22 ogólnego rozporządzenia o ochronie danych osobowych.

**PREZES ZARZĄDU**

*mgr inż. Edward Jankowski*