Załącznik nr 2
do Regulaminu udzielania
Zamówień Publicznych w MZZDiOŚ

ZAPYTANIE OFERTOWE

Miejski Zakład Zieleni, Dróg i Ochrony Środowiska w Kołobrzegu zwraca się z prośbą o przedstawienie swojej oferty na poniżej opisany przedmiot zamówienia:

„**Przeprowadzenie audytu wstępnego (diagnostycznego) oraz przegląd, opracowanie, aktualizację oraz wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz przeprowadzenie audytu SZBI.**"

<u>Opis przedmiotu zamówienia:</u>

1. Zamówienie obejmuje wykonanie następujących zadań:
    a. **Zadanie 1**: Przeprowadzenie audytu wstępnego oraz przegląd wraz z aktualizacją i wdrożeniem dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).
    b. **Zadanie 2**: Przeprowadzenie audytu SZBI zgodnego w wymaganiami Ustawy o Krajowym Systemie Cyberbezpieczeństwa.
    c. **Zadanie 3**.: Przeprowadzenie szkolenia z zakresu Cyberbezpieczeństwa pracowników Zamawiającego.
2. **Zadanie 1: Przeprowadzenie audytu wstępnego oraz przegląd wraz z aktualizacją i wdrożeniem dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).**
    a) W ramach pierwszego etapu Zadania 1 Wykonawca dokona identyfikacji rodzaju podmiotu Zamawiającego na podstawie Ustawy o KSC oraz zapewni wsparcie w przygotowaniu informacji niezbędnych do dokonania zgłoszenia do wykazu podmiotów kluczowych i ważnych.
    b) W ramach drugiego etapu Zadania 1 Wykonawca przeprowadzi audyt wstępny funkcjonującego Systemu Zarządzania Bezpieczeństwem Informacji w siedzibie Zamawiającego oraz w dwóch podległych jednostkach, tj. RIPOK oraz Cmentarz Komunalny, wraz z analizą ryzyka, wymaganą przez ustawę o KSC. Audyt wstępny będzie uwzględniał

analizę zgodności w obszarach takich jak: polityki bezpieczeństwa informacji, zarządzanie ryzykiem, kontrola dostępu, kryptografia, bezpieczeństwo fizyczne, eksploatacja systemów, relacje z dostawcami, incydenty, ciągłość działania oraz ocenę skuteczności wdrożonych środków technicznych w tych obszarach.

c) Wykonawca przedstawi Zamawiającemu zbiorczy raport z przeprowadzonego audytu bezpieczeństwa wraz z rekomendacjami, oceną ryzyka oraz propozycjami działań naprawczych i doskonalących.

d) W ramach trzeciego etapu Zadania 1 Wykonawca odpowiednio zaktualizuje/opracuje dokumentację Systemu Zarządzania Bezpieczeństwem na podstawie wyników audytu, co do wymagań ustawy o KSC. Dokumentacja musi obejmować m.in. polityki, role, ryzyko, zarządzanie incydentami, postęp, pracę zdalną, bezpieczeństwo fizyczne, kopie zapasowe, monitoring, relacje z dostawcami.

Zamawiający wymaga przekazania zaktualizowanego zestawu dokumentacji w wersji edytowalnej (.docx, .xlsx) oraz PDF.

3. **Zadanie 2: Przeprowadzenie audytu SZBI zgodnego z wymaganiami Ustawy o Krajowym Systemie Bezpieczeństwa.**

a) W ramach Zadania nr 2 Wykonawca dokona audytu zgodnie z wymaganiami ustawy o KSC. Na podstawie przeprowadzonej analizy dokumentacji oraz audytu bezpieczeństwa, Wykonawca jest zobowiązany przedstawić pisemny raport zawierający wszystkie wyniki, wnioski wraz z propozycją zmian w zakresie spełnienia wymagań Rozporządzenia KRI. W raporcie muszą zostać uwzględnione wszystkie wyniki cząstkowe z audytowanych obszarów. Spełnienie poszczególnych wymagań zostanie określone w trzyelementowej skali: 1) spełnione – oznacza, że wymaganie normy zostało całkowicie wdrożone, 2) częściowo spełnione – może zaistnieć, czy dany obszar został udokumentowany (opracowano stosowną procedurę lub przygotowano inne zabezpieczenie), ale wybrany mechanizm nie został skutecznie wdrożony (np. zdefiniowano strefy bezpieczeństwa, ale system kontroli dostępu nie funkcjonuje poprawnie); najczęstszym przypadkiem oznaczenia wymagania jako „częściowo spełnionego" jest nieskuteczne wdrożenie procedury (nie przestrzeganie zapisów procedury przez pracowników), 3) niespełnione – wymaganie niespełnione oznacza, że nie zostało ono w ogóle zidentyfikowane przez podmiot (podmiot nie jest świadomy danego zagrożenia) lub nie podjęto żadnych działań, aby wdrożyć odpowiednie mechanizmy zabezpieczające.

4. **Zadanie 3: Przeprowadzenie szkolenia z zakresu Cyberbezpieczeństwa pracowników Zamawiającego.**

   a) W ramach Zadania nr 3 Wykonawca przeprowadzi szkolenie pracowników umysłowych Zamawiającego w zakresie bezpieczeństwa informacji i wymogów w zakresie cyberbezpieczeństwa. Celem szkolenia jest zwiększenie świadomości pracowników Zamawiającego w zakresie problematyki związanej z bezpieczeństwem informacji, umiejętności strategicznego zarządzania cyberbezpieczeństwem oraz zrozumienie przepisów prawnych i ich implementacji. Szkolenie musi obejmować co najmniej problematykę:

   - Podstawy cyberbezpieczeństwa (podstawowe pojęcia i zasady działania),
   - Przegląd najpopularniejszych zagrożeń (w tym rodzaje ataków, ransomwarei malware, phishing, oszustwa i wyłudzenia z uwzględnieniem oszustwa typu Business E-mail Compromise, atak telefoniczny, spoofing, atak odwrócony – zmuszenie ofiary do szukania pomocy u atakującego, przekręt nigeryjski, wyłudzenia BLIK, oszustwo na dyrektora/prezesa),
   - Znaczenie cyberbezpieczeństwa dla Spółki
   - Przegląd aktualnych zagrożeń i trendów w cyberprzestrzeni

   b) Szkolenie musi być przeprowadzone stacjonarnie, w siedzibie Zamawiającego.

   c) Miejsce szkolenia: siedziba Zamawiającego. Zamawiający udostępni salę konferencyjną wraz z projektorem oraz zapewni dostęp do Internetu.

   d) Liczba osób do przeszkolenia: do 45.

   e) Szkolenie musi zostać przeprowadzone w trzech grupach. Minimalny czas szkolenia dla każdej z grup: 2 godziny.

   f) Po przeprowadzeniu szkolenia Wykonawca przedstawi Zamawiającemu imienną listę osób przeszkolonych, zawierającą podpis osoby przeszkolonej.

<u>Termin wykonania zamówienia:</u>

1. Termin realizacji Zadania 1: do 60 dni od dnia zawarcia umowy
2. Termin realizacji Zadania 2: do 30 dni od dnia powiadomienia Wykonawcy przez Zamawiającego o gotowości do przeprowadzenia audytów – przewidywany termin realizacji październik-listopad 2026
3. Termin realizacji Zadania 3: do ustalenia, preferowany październik-listopad 2026 r.

<u>Warunki udziału w postępowaniu:</u>

1. O udzielenie zamówienia mogą ubiegać się wykonawcy, spełniający poniższe warunki:

a) wykażą, że w ciągu ostatnich 3 latach przed terminem składania ofert wykonali należycie co najmniej dwa zamówienia polegające na opracowaniu lub przeglądzie i aktualizacji Systemu Zarządzania Bezpieczeństwem Informacji.
b) dysponują co najmniej jednym audytorem, który będzie uczestniczyć w realizacji zamówienia, który:
    a. ma wykształcenie wyższe.
    b. posiada co najmniej dwuletnie doświadczenie polegające na opracowaniu lub przeglądzie i aktualizacji Systemu Zarządzania Bezpieczeństwem Informacji
    c. posiada co najmniej dwuletnie doświadczenie w prowadzeniu audytów cyberbezpieczeństwa

Kryterium oceny ofert:

Cena 100 %

Ofertę wraz z wypełnionymi i podpisanymi następującymi oświadczeniami:
- oświadczenie o spełnianiu warunków udziału w postepowaniu, aktualne na dzień składania ofert

- świadczenie o braku podstaw do wykluczenia z postępowania składane na podstawie ustawy z 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego

prosimy przesłać pocztą elektroniczną na adres: **r.michalczyk@zielen.kolobrzeg.pl**
Termin składania ofert: 01.06.2026 r.

.....
(podpis osoby prowadzącej postępowanie)