Cyberbezpieczne Wodociągi

ZAPYTANIE OFERTOWE

Nr postępowania: MPWiK/2/2026/C

Dotyczy zamówienia pn.:

„Opracowanie, wdrożenie, przegląd i aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), opracowanie planów ciągłości działania (BCP) i odtwarzania po awarii (DRP) dla systemów teleinformatycznych (STI), opracowanie i wdrożenie Systemu Zarządzania Ciągłością Działania (SZCD), przeprowadzenie audytów cyberbezpieczeństwa, organizacja i przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa oraz wykonanie testów bezpieczeństwa infrastruktury sieciowej w środowiskach IT/OT/ICS/IIoT w ramach projektu „Wzmocnienie cyberbezpieczeństwa sieci w MPWiK w Łasku Sp. z o.o.”

1. Zamawiający

Miejskie Przedsiębiorstwo Wodociągów i Kanalizacji w Łasku Sp. z o.o.
ul. Tylna 9 98-100 Łask NIP: 831-15-06-734 REGON: 731020519 KRS: 0000065222

2. Informacje ogólne o postępowaniu

Postępowanie prowadzone jest w celu wyboru wykonawcy dla zamówienia obejmującego opracowanie, wdrożenie, przegląd i aktualizację Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), opracowanie planów ciągłości działania (BCP) oraz planów odtwarzania po awarii (DRP) dla systemów teleinformatycznych (STI), opracowanie i wdrożenie Systemu Zarządzania Ciągłością Działania (SZCD), przeprowadzenie audytów cyberbezpieczeństwa, a także organizację i przeprowadzenie specjalistycznych szkoleń z zakresu cyberbezpieczeństwa oraz wykonanie testów bezpieczeństwa infrastruktury sieciowej w środowiskach IT/OT/ICS/IIoT.

Zamówienie realizowane jest w ramach projektu: **„Wzmocnienie cyberbezpieczeństwa sieci w MPWiK w Łasku Sp. z o.o.”** (konkurs grantowy „Cyberbezpieczne Wodociągi”).

3. Podstawa prawna i tryb prowadzenia postępowania

Szacunkowa wartość niniejszego zamówienia nie przekracza kwoty 170 000,00 zł netto. W związku z powyższym, zgodnie z art. 2 ust. 1 pkt 1 ustawy z dnia 11 września 2019 r. – Prawo zamówień

publicznych (t.j. Dz.U. z 2024 r. poz. 1320 z późn. zm.), **do niniejszego postępowania nie stosuje się przepisów tej ustawy**.

Postępowanie prowadzone jest w trybie zapytania ofertowego zgodnie z Zasadą Konkurencyjności. Oferty należy składać w terminie i w sposób określony w niniejszym postępowaniu wyłącznie za pośrednictwem Bazy Konkurencyjności (BK2021).

Celem postępowania jest wybór wykonawcy posiadającego odpowiednie kwalifikacje i doświadczenie w realizacji usług z zakresu cyberbezpieczeństwa, w szczególności w obszarze systemów zarządzania bezpieczeństwem informacji, ciągłości działania, audytów bezpieczeństwa, testów infrastruktury teleinformatycznej oraz prowadzenia szkoleń specjalistycznych.

4. Szczegółowy zakres zamówienia

Przedmiot zamówienia został podzielony na następujące elementy i obejmuje w szczególności:

I. Szkolenia z zakresu cyberbezpieczeństwa:

1. Podstawowe szkolenia budujące świadomość cyberzagrożeń oraz sposobów ochrony dla pracowników IT/OT/ICS.
2. Szkolenia dla kadry kierowniczej, istotne z punktu widzenia wdrażanej polityki bezpieczeństwa informacji oraz systemu zarządzania bezpieczeństwem informacji IT/OT/ICS.
3. Szkolenia specjalistyczne dla informatyka w zakresie zastosowanych (lub planowanych do zastosowania) środków bezpieczeństwa w ramach Projektu grantowego IT/OT/ICS oraz szkolenia przygotowujące do certyfikacji z zakresu cyberbezpieczeństwa IT/OT/ICS.
4. Szkolenia powiązane z testami socjotechnicznymi, które będą weryfikować świadomość zagrożeń oraz reakcje personelu, w szczególności reagowanie specjalistów posiadających odpowiednie obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami IT/OT/ICS.

II. Systemy Zarządzania i Plany Ciągłości Działania:

5. Opracowanie, wdrożenie, przegląd, aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), planów ciągłości działania (BCP) i odtwarzania po awarii (DRP) dla systemów teleinformatycznych (STI).
6. Opracowanie, wdrożenie, przegląd, aktualizacja Systemu Zarządzania Ciągłością Działania STI (SZCD).

III. Audyty i Testy Bezpieczeństwa:

7. **U02.** Testy bezpieczeństwa infrastruktury sieciowej IT/OT/ICS/IIoT.

8. Audyt SZBI, audyt SZCD, audyt zgodności z KRI/uoKSC (przeprowadzony przez wykwalifikowanych audytorów) oraz audyt (re)certyfikacji SZBI i SZCD na zgodność z normami dla środowisk IT/OT/ICS.

Szczegółowy zakres techniczny zamówienia, wymagania wobec wykonawców oraz warunki realizacji zamówienia zostały określone w dalszej części dokumentacji postępowania.

Szczegółowy usług objętych przedmiotem zamówienia przedstawiono poniżej:

1. **Szkolenia z zakresu cyberbezpieczeństwa - podstawowe szkolenia budujące świadomość cyberzagrożeń oraz sposobów ochrony dla pracowników IT/OT/ICS**

Przedmiotem zamówienia jest przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa.

Szkolenie musi być zrealizowane w siedzibie Zamawiającego.

W ramach szkolenia, uczestnicy muszą otrzymać konkretne porady do zastosowania w praktyce, tak aby możliwe było ich sprawne i zarazem bezpieczne funkcjonowanie w cyberprzestrzeni.

Program kursu musi skupiać się na najważniejszych w danym obszarze aspektach. Trenerzy muszą zapewnić wysoki poziom merytoryczny oraz komunikacyjny. Szkolenie ma zapoznać uczestnika z zagrożeniami, technikami ataków cyberprzestępczych oraz metodami socjotechnicznymi, ukierunkowanymi na osoby pracujące na co dzień przed komputerem. Uczestnicy mają dowiedzieć się jak działa rynek cyberprzestępczy, jakimi kwotami operują współcześni przestępcy, jakimi sposobami próbują uzyskać dostęp do sieci teleinformatycznej oraz jak w czasie rozmowy osobistej, telefonicznej lub mailowej oszuści potrafią wyłudzić informację od nieświadomego pracownika. Podczas szkolenia uczestnik ma być również edukowany ze skutków, dla których wykorzystywanie komputera służbowego do celów prywatnych zwiększa ryzyko ataku na całą organizację.

Szkolenie musi być skierowane do każdego pracownika w organizacji bez względu na jego wiedzę i umiejętności informatyczne.

Korzyści po szkoleniu:

- zdobycie wiedzy obejmującej bezpieczne zarządzanie miejscem pracy oraz danymi
- zdobycie wiedzy umożliwiającej ochronę przed atakami socjotechnicznymi

Wykonawca zobowiązany jest do:

- wydania imiennych zaświadczeń / certyfikatów dla każdego uczestnika,
- zapewnienia dla każdego uczestnika materiałów szkoleniowych w formie elektronicznej.

Zakres merytoryczny szkolenia:

- Co to jest cyberprzestępczość?
- Opis funkcjonowania zorganizowanych grup cyberprzestępczych
- Czy jestem atrakcyjnym „klientem” dla cyberprzestępcy?
- Jakie zyski może mieć cyberprzestępca atakując moje dane?
- Straty wynikające z udanego ataku
- Rodzaje ataków skierowane w użytkowników Internetu
- Jak bronić się przed cyberprzestępcami?
- Spam jako niegroźny sposób na groźne ataki • Handel adresami e-mail
- Kampanie Phishingowe
- Opłacalność ataków DoS/DDoS wymierzonych w konkretną instytucję
- Groźne ataki 0-day
- Nieopłacona FV jako sposób przemycenia wirusa do naszego komputera
- Ataki socjotechniczne - czyli niewinne „wyłudzanie” danych
- Przekazywanie haseł dostępowych znajomym
- Fizyczne bezpieczeństwo danych osobowych
- Znaleziony pendrive na parkingu jako pozwolenie na atak dla cyberprzestępcy
- Aktualne zagrożenia wynikające z wojny w Ukrainie
- Podsumowanie szkolenia, pytania, dyskusja

2. **Szkolenia z zakresu cyberbezpieczeństwa - szkolenia dla kadry, istotne z punktu widzenia wdrażanej polityki bezpieczeństwa informacji oraz systemu zarządzania bezpieczeństwem informacji IT/OT/ICS**

W ramach realizacji usługi Wykonawca przeprowadzi szkolenia dla zespołu ds. SZBI, powołanego przez Zamawiającego, w którym omówione zostaną zasady funkcjonowania i utrzymania systemu zarządzania bezpieczeństwem informacji (SZBI).

Szkolenie z wdrażania udokumentowanego Systemu Zarządzania Bezpieczeństwem Informacji przygotowuje do zarządzania bezpieczeństwem w oparciu o normę ISO 27001, obejmując analizę kontekstu organizacji, szacowanie ryzyka, wybór i wdrażanie zabezpieczeń, tworzenie dokumentacji (polityk, procedur, instrukcji), a także audytowanie i ciągłe doskonalenie systemu w celu ochrony informacji przed zagrożeniami, zgodnie z wymaganiami prawnymi.

Główne cele szkolenia:

- Zrozumienie wymagań normy ISO/IEC 27001 - dogłębna analiza punktów normy, terminologii, celów bezpieczeństwa informacji, zasad przywództwa, planowania i funkcjonowania SZBI;

- Praktyczne umiejętności - nauka identyfikacji aktywów informacyjnych, analizy i oceny ryzyka (np. metodą PDCA), projektowania i wdrażania zabezpieczeń;
- Tworzenie dokumentacji - ćwiczenia z tworzenia polityki bezpieczeństwa, procedur, instrukcji i deklaracji stosowania.
- Rola pełnomocnika ds. SZBI oraz audytora wewnętrznego - wyjaśnienie roli koordynatora lub pełnomocnika SZBI, a także audytorów wewnętrznych.
- Aspekty prawne i organizacyjne - uwzględnienie wymagań prawnych (np. dyrektywy NIS 2), kontekstu organizacji, oczekiwań interesariuszy oraz roli zasobów ludzkich.

Minimalny program szkolenia:

- Wprowadzenie - definicje, zakres SZBI, rola dokumentacji (polityki, procedury);
- Kontekst organizacji - analiza otoczenia, identyfikacja interesariuszy;
- Przywództwo - wymagania dla kierownictwa;
- Planowanie - ustalanie celów, podejście oparte na ryzyku;
- Wsparcie - zasoby, kompetencje, komunikacja, dokumentacja;
- Funkcjonowanie - realizacja procesów, identyfikacja i ocena ryzyka;
- Ocena wyników - monitorowanie, pomiary, audyty wewnętrzne;
- Doskonalenie - działania korygujące i zapobiegawcze.
- Zabezpieczenia organizacyjne, osobowe, fizyczne i technologiczne
- Ćwiczenia praktyczne - identyfikacja ryzyka, tworzenie i przegląd dokumentów.

Wymiar szkolenia: co najmniej 4 godziny zegarowe na turę.

3. **Szkolenia z zakresu cyberbezpieczeństwa - szkolenia specjalistyczne dla informatyka w zakresie zastosowanych (planowanych do zastosowania) środków bezpieczeństwa w ramach Projektu grantowego IT/OT/ICS / Szkolenia przygotowujące do certyfikacji z zakresu cyberbezpieczeństwa IT/OT/ICS.**

Przedmiotem zamówienia jest dostarczenie vouchera dla 1 osoby na autoryzowane szkolenie Microsoft MS-55371 Windows Server Administration oraz Microsoft MS-55376 Installation, Storage, and Compute with Windows Server. Prowadzącym szkolenie musi być autoryzowany trener Microsoft.

4. **Szkolenia z zakresu cyberbezpieczeństwa - szkolenia powiązane z testami socjotechnicznymi, które będą weryfikować świadomość zagrożeń oraz reakcje personelu, w szczególności reagowanie specjalistów posiadających odpowiednie obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami IT/OT/ICS**

Przeprowadzenie kampanii phishingowej oraz przygotowanie raportu zawierającego wyniki z analizą kampanii.

a) wybór domeny (łudząco podobnej do prawdziwych domen Zamawiającego), która zostanie wykorzystana do kampanii phishingowej;
b) opracowanie bazy mailingowej pracowników objętych kampanią phishingową oraz spreparowanego dokumentu zbliżonego wyglądem do dokumentów Zamawiającego, zawierającego dodatkowy niezłośliwy kod pozwalający na mierzenie efektów kampanii;
c) wyznaczenie osób wtajemniczonych w fakt przeprowadzania testów (np. najwyższe kierownictwo, dział informatyczny lub wyłącznie szef tego działu, inspektor ochrony danych lub inna osoba odpowiedzialna za bezpieczeństwo w organizacji);
d) dodanie domeny wybranej do przeprowadzenia kampanii phishingowej do tzw. białej/zaufanej listy w celu pominięcia filtrów antyspamowych (celem testu jest dostarczenie spreparowanej wiadomości na wszystkie skrzynki pracowników i weryfikacja ich podatności na prawdziwe kampanie cyberprzestępców);
e) przeprowadzenie kampanii phishingowej (wysłanie przygotowanej uprzednio wiadomości e mail do pracowników wskazanych w bazie mailingowej)
f) raport z testu phishingowego.

Testy muszą być zrealizowane w wymiarze co najmniej 7 dni roboczych (tj. 16 godzin).

Przeprowadzenie prób ataków socjotechnicznych polega na wywieraniu wpływu na ludzi i stosowaniu perswazji w celu oszukania ich tak, aby uwierzyli, że socjotechnik jest osobą o sugerowanej przez siebie, a stworzonej na potrzeby manipulacji, tożsamości. Dzięki temu socjotechnik jest w stanie wykorzystać swoich rozmówców, przy dodatkowym (lub nie) użyciu środków technologicznych, do zdobycia poszukiwanych informacji. Przeprowadzane próby w Organizacji będą miały na celu zweryfikowanie świadomości pracowników i zabezpieczeń przed atakami socjotechnicznymi.

Testy muszą składać się z następujących faz:

- Rozpoznanie (biały wywiad, obserwacja pracy pracowników).
- Budowanie więzi i zaufania (użycie wewnętrznych informacji, podawanie się za kogoś innego, wspominanie nazwisk osób znanych ofierze, zgłoszenie potrzeby pomocy lub zasugerowanie posiadania władzy).
- Wykorzystanie zaufania (prośba o informację lub działanie skierowana do ofiary).

Testy muszą być przeprowadzone za pomocą aktualnych narzędzi, wykorzystujących najnowsze możliwości w zakresie symulacji złośliwych kampanii socjotechnicznych.

Zakres testów:

- Ataki typu phishing,
- Ataki typu spear phishing
- Phishing typu whaling
- Phishing przez klonowanie

- Angler phishing

Wykonawca zobowiązany jest do wykrycia (w stosunku do konkretnego adresu email):

- otwieranych wiadomości,
- otwierania plików w popularnych formatach, takich jak „docx.", czy „xlsx".
- otwieranych stron za pomocą linków umieszczonych w wiadomościach,
- podawanych poświadczeń na stronach mających na celu wyłudzanie informacji, przygotowanych przez testerów.

Po wykonanych testach Wykonawca jest zobowiązany omówić ich wyniki z personelem Zamawiającego.

5. **Opracowanie, wdrożenie, przegląd, aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), planów ciągłości działania (BCP) i odtwarzania po awarii (DRP) dla STI**

Wykonawca jest zobowiązany do wdrożenia u Zamawiającego kompleksowego SZBI, obejmującego polityki, procedury, działania, role, kompetencje i procesy mające na celu zarządzanie ryzykiem związanym z bezpieczeństwem informacji.

SZBI musi być dopasowany do realiów operacyjnych Zamawiającego oraz charakterystyki jego systemów IT i OT. SZBI musi objąć również plany ciągłości działania systemów oraz proces szacowania ryzyka. W pierwszym kroku musi zostać wykonany audyt przedwdrożeniowy względem wymagań KRI, UoKSC, aby precyzyjnie określić braki organizacyjne, kompetencyjne i techniczne oraz ustalić priorytety i harmonogram działań. Przeprowadzone musi zostać również szacowanie ryzyka (na podstawie ISO/IEC 27005), obejmujące inwentaryzację aktywów, identyfikację zagrożeń i podatności, ocenę prawdopodobieństwa i skutków oraz opracowanie planu postępowania z ryzykiem.

W ramach przygotowania dokumentacji SZBI Wykonawca zobowiązany jest do uwzględnienia aspektów związanych z bezpieczeństwem fizycznym, technologicznym, osobowym i organizacyjnym, takich jak:

- ochrona obiektów, sprzętu, infrastruktury technicznej oraz personelu przed zagrożeniami, takimi jak kradzież, sabotaż czy nieuprawniony dostęp;
- ochrona systemów teleinformatycznych przed atakami cybernetycznymi, nieautoryzowanymi zmianami, awariami oraz błędami ludzkimi;
- ochrona informacji przed zagrożeniami osobowymi obejmującymi pracowników Zamawiającego oraz personel dostawców/partnerów.

SZBI musi obejmować minimum następujące obszary:

a) ustanowienie polityki bezpieczeństwa informacji oraz polityk tematycznych, w tym polityk analizy ryzyka i bezpieczeństwa systemów informatycznych;
b) aktualizacje regulacji wewnętrznych w zakresie bezpieczeństwa informacji;
c) utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji;
d) opracowanie polityk i procedur służących ocenie skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie;
e) przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji;
f) bezpieczeństwo zasobów ludzkich, polityka kontroli dostępu i zarządzanie aktywami;
g) podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia;
h) zapewnienie szkoleń osób zaangażowanych w proces przetwarzania informacji, w tym przeprowadzanie szkoleń w zakresie cyberbezpieczeństwa;
i) zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami;
j) ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
k) zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionym osobom jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
l) opracowanie polityk i procedur stosowania kryptografii;
m) bezpieczeństwo łańcucha dostaw, w tym aspekty związane z bezpieczeństwem dotyczące stosunków między Zamawiającym, a jego bezpośrednimi dostawcami, usługodawcami i poddostawcami;
n) zawierania w umowach serwisowych, podpisanych ze stronami trzecimi, zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
o) ciągłość działania kluczowych usług, w tym zarządzanie kopiami zapasowymi i przywracanie normalnego działania po wystąpieniu sytuacji nadzwyczajnej oraz zarządzanie kryzysowe;
p) stosowanie uwierzytelniania wieloskładnikowego oraz ciągłych, zabezpieczonych połączeń głosowych, tekstowych i wideo oraz zabezpieczonych systemów łączności wewnątrz podmiotu w sytuacjach nadzwyczajnych;
q) zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, w tym bezpieczeństwo w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych oraz postępowanie w przypadku wykrycia podatności i ich ujawnianie;
r) zarządzanie incydentami bezpieczeństwa informacji i cyberbezpieczeństwa;
s) zapewnienia okresowego audytu w zakresie bezpieczeństwa informacji.

Dokumentacja musi uwzględniać wymagania następujących aktów prawnych oraz norm:

- Ustawa o Krajowym Systemie Cyberbezpieczeństwa;
- Norma PN-EN ISO/IEC 27001:2023;
- Norma PN-EN ISO/IEC 27002:2023;
- Rozporządzenie 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;
- Rozporządzenie 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;
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Tekst mający znaczenie dla EOG)

Wykonawca ma obowiązek przekazać Zamawiającemu:

- pełną dokumentację systemu zarządzania bezpieczeństwem informacji;
- zalecenia mające na celu zwiększenie poziomu bezpieczeństwa informacji Zamawiającego.

6. **Opracowanie, wdrożenie, przegląd, aktualizacja Systemu Zarządzania Ciągłością Działania STI (SZCD)**

Wykonawca jest zobowiązany do wdrożenia u Zamawiającego kompleksowego SZCD, obejmującego polityki, procedury, działania, role, kompetencje i procesy mające na celu zarządzanie ryzykiem związanym z zakłóceniami ciągłości działania.

SZCD musi być dopasowany do realiów operacyjnych Zamawiającego oraz charakterystyki jego systemów IT i OT. W pierwszym kroku musi zostać wykonany audyt przedwdrożeniowy względem wymagań ISO 22301 aby precyzyjnie określić braki organizacyjne, kompetencyjne i techniczne oraz ustalić priorytety i harmonogram działań.

W ramach wdrożenia należy:

- opracować proces identyfikacji, dostępu i oceny obowiązujących wymogów prawnych i regulacyjnych,
- określić zakres SZCD,
- stworzyć politykę ciągłości działania,
- opracować cele SZCD,

- zaprojektować proces identyfikacji niezbędnych kompetencji, ich zdobywania i rozwoju,
- opracować procedury zarządzania udokumentowanymi informacjami,
- opracować analizę wpływu na biznes i ocenę ryzyka wystąpienia zakłóceń,
- stworzyć procedury kierowania działaniami zespołu w strukturze reagowania,
- opracować procedury ostrzegania i komunikacji,
- stworzyć plany i procedury dotyczące ciągłości działania,
- określić procesy przywracania i odtwarzania działalności biznesowej ze środków tymczasowych przyjętych w trakcie i po zakończeniu zakłócenia,
- opracować proces wykonywania ćwiczeń w zakresie ciągłości działania,
- stworzyć procedury monitorowania, pomiaru, analizy i oceny SZCD,
- opracować proces audytów wewnętrznych w zakresie SZCD,
- stworzyć zasady wykonywania przeglądów zarządzania,
- opracować procedury zarządzania niezgodnościami i działaniami korygującymi.

Dokumentacja musi uwzględniać wymagania następujących aktów prawnych oraz norm:

- Ustawa o Krajowym Systemie Cyberbezpieczeństwa;
- Norma PN-EN ISO/IEC 22301;
- Rozporządzenie 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;
- Rozporządzenie 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;
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Tekst mający znaczenie dla EOG)

Wykonawca ma obowiązek przekazać Zamawiającemu:

- pełną dokumentację systemu zarządzania ciągłością działania;
- zalecenia mające na celu zwiększenie poziomu bezpieczeństwa informacji Zamawiającego.

7. Testy bezpieczeństwa infrastruktury sieciowej IT/OT/ICS/IIoT

Usługa testowania bezpieczeństwa obejmuje skanowanie podatności testowanego środowiska, przeprowadzona zgodnie z założeniem że zespół testujący przystępując do realizacji testów ma wiedzę o przedmiocie testów na poziomie analogicznym jak inni jej użytkownicy.

Raport z testów musi wyszczególniać zakres przeprowadzonych testów oraz wszystkie wyniki ze szczególnym uwzględnieniem potencjalnych skutków wpływu zmaterializowania się zagrożenia, wskazanie środków które wpłyną na poprawę stanu zabezpieczenia systemu oraz szczegóły techniczne wykrytych podatności wraz z określeniem poziomu ich istotności.

Celem przeprowadzenia testów podatności systemu teleinformatycznego ma być zidentyfikowanie słabych punktów bezpieczeństwa, opierając się na zidentyfikowanych podatnościach.

Testy muszą obejmować hosty w sieci wewnętrznej oraz dostępne z poziomu sieci publicznej w wyznaczonych adresacjach. Dodatkowo wykonawca musi przeprowadzić analizę topologii sieci wraz z próbami wykrycia nieszczelności w skonfigurowanych urządzeniach.

Testy muszą składać się z następujących faz:

- Faza rozpoznania - rozpoznanie aktywne obejmuje działania mające na celu zebranie informacji o testowanym systemie. Aktywność testującego opiera się na bezpośredniej interakcji ze środowiskiem celu. Zawiera w sobie działania takie jak skanowanie portów, wykrywanie usług czy hostów działających w sieci.
- Faza oceny podatności sieci wewnętrznej oraz urządzeń dostępnych z poziomu sieci internet: analiza występowania w badanym systemie podatności zawartych w bazach danych podatności, ocena wykorzystania skompromitowanych protokołów, weryfikacja słabości systemu na popularne ataki, próby eksploatacji wykrytych podatności technicznych,
- Przygotowanie raportu z oceny wraz z zaleceniami działań naprawczych.

Testy muszą być przeprowadzone przez aktualne narzędzia wykorzystujące najnowsze bazy podatności.

Zakres testów:

- testy bezpieczeństwa sieci teleinformatycznych w tym brzegu sieci,
- testy bezpieczeństwa baz danych,
- testy bezpieczeństwa środowisk serwerowych w tym systemów operacyjnych,
- testy bezpieczeństwa środowisk wirtualnych,

- konsultacje z zamawiającym.

Wykonawca zobowiązany jest do:

- wykrycia działających usług w systemie teleinformatycznym,
- wykrycia otwartych portów na poszczególnych urządzeniach,
- zidentyfikowania podatności na poszczególnych hostach,
- wyszukania błędów konfiguracyjnych,
- określenia stopnia istotności wykrytych podatności technicznych,
- opracowania raportu podsumowującego z zaleceniami działań naprawczych.

8. Audyt SZBI, audyt SZCD, audyt zgodności KRI/uoKSC przez wykwalifikowanych audytorów, audyt (re)certyfikacji SZBI, SZCD na zgodność z normami IT/OT/ICS

Przedmiotem zamówienia jest usługa wykonania audytu zgodności, którego kryterium jest Rozporządzenie 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 (zwanym dalej „Rozporządzeniem KRI") oraz Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (zwana dalej „UoKSC").

Audyt musi być przeprowadzony przez co najmniej trzech audytorów posiadających uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.

Audyt musi być zrealizowany w siedzibie Zamawiającego, w wymiarze co najmniej 1 dnia roboczego (tj. 8 godzin).

Audyt ma obejmować weryfikację bezpieczeństwa fizycznego (sprawdzenie ochrony pomieszczeń, sprzętów, infrastruktury oraz personelu przed bezpośrednim działaniem czynników fizycznych i zdarzeń takich jak kradzież, nieuprawniony dostęp), bezpieczeństwa informatycznego (analiza bezpieczeństwa systemu teleinformatycznego) oraz bezpieczeństwa organizacyjnego i osobowego (stosowane procedury bezpieczeństwa), w tym przegląd dokumentacji dotyczącej systemu zarządzania bezpieczeństwem informacji.

Audyt musi obejmować weryfikację:

a) systemu zarządzania bezpieczeństwem informacji,
b) zapewnienia aktualizacji regulacji wewnętrznych w zakresie bezpieczeństwa informacji,
c) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji,

d) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji,
e) podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia,
f) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji,
g) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami,
h) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość,
i) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie,
j) zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji,
k) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży,
l) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych,
m) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji,
n) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji.

Kryteriami audytu są:

- Rozporządzenie 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;
- Ustawa o Krajowym Systemie Cyberbezpieczeństwa;
- Norma ISO/IEC 27001;
- Norma ISO 22301;
- Dyrektywa NIS 2.

Wykonawca zobowiązany jest do dostarczenia Zamawiającemu:

- rekomendacji do wdrożenia w celu poprawy cyberbezpieczeństwa Zamawiającego,
- raportu z audytu.

5. Wymagania wobec Wykonawcy

Zdolność techniczna:

a) W okresie 5 lat poprzedzających złożenie oferty Wykonawca należycie przeprowadził co najmniej 3 audyty bezpieczeństwa systemów teleinformatycznych, w tym co najmniej jeden z testami penetracyjnymi, na rzecz podmiotów realizujących zadania publiczne, z których każdy miał wartość nie mniejszą niż 50 000,00 zł brutto, co potwierdzono stosownymi referencjami.
b) Wykonawca należycie zrealizował co najmniej 4 inne audyty cyberbezpieczeństwa (niewskazane w pkt. a i c) dla podmiotów realizujących zadania publiczne, z których każdy miał wartość nie mniejszą niż 20 000,00 zł brutto, co zostało udokumentowane referencjami.
c) Wykonawca przeprowadził co najmniej 15 innych audytów bezpieczeństwa informacji (niewskazanych w pkt. a i b).
d) W okresie 5 lat poprzedzających złożenie oferty Wykonawca należycie wykonał co najmniej 2 usługi przeprowadzenia szkoleń z zakresu cyberbezpieczeństwa dla podmiotów realizujących zadania publiczne, z których każda miała wartość nie mniejszą niż 20 000,00 zł brutto, co zostało udokumentowane referencjami.
e) Wykonawca należycie opracował dokumentację systemu zarządzania bezpieczeństwem informacji dla minimum 5 podmiotów realizujących zadania publiczne, co potwierdzono stosownymi referencjami.
f) Wykonawca należycie zrealizował co najmniej 2 projekty dotyczące szacowania ryzyka związanego z bezpieczeństwem danych w systemach informatycznych dla podmiotów realizujących zadania publiczne, co zostało potwierdzone stosownymi referencjami.

Zdolność zawodowa

Wykonawca posiada zespół skierowany do realizacji przedmiotu zamówienia składający się z co najmniej 3 osób, w tym:

a) minimum 3 osób posiadających ważne certyfikaty audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 lub równoważnej, wydane przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób;
b) minimum 2 osób posiadających wiedzę i doświadczenie w obszarze audytów systemów zarządzania bezpieczeństwem informacji przy spełnieniu wymagań dla audytorów IRCA, CQI, potwierdzonych certyfikatem lub równoważnym dokumentem ukończenia kursu Information Security Management Systems (ISMS) Auditor;
c) minimum 1 osoba w zespole musi posiadać wiedzę i doświadczenie w zakresie wdrażania systemów zarządzania bezpieczeństwem informacji zgodnych z normą ISO 27001 lub równoważnych standardów o zbliżonym poziomie jakości. Wymagane jest potwierdzenie kwalifikacji ważnym certyfikatem lub równoważnym dokumentem ukończenia szkolenia w tym obszarze. Ponadto osoba ta musi posiadać doświadczenie w realizacji wdrożeń systemu zarządzania bezpieczeństwem informacji realizowanych w co najmniej 5 podmiotach publicznych;

d) minimum 1 osoba z kwalifikacjami w zakresie audytowania systemów zarządzania ciągłością działania, potwierdzonymi spełnieniem wymagań dla audytorów wiodących systemu zarządzania ciągłością działania zgodnego z normą PN-EN ISO 22301, lub równoważną, potwierdzone certyfikatem dla audytora wiodącego systemu zarządzania ciągłością działania zgodnego z normą PN-EN ISO 22301 po zdaniu egzaminu;
e) minimum 1 osobę posiadającą wiedzę i doświadczenie w zakresie wdrażania systemu zarządzania ciągłością działania wg ISO 22301 potwierdzoną ważnym certyfikatem lub równoważnym dokumentem ukończenia szkolenia w tym zakresie;
f) przynajmniej 2 osoby posiadające kompetencje w zakresie audytowania systemów zarządzania jakością przy spełnieniu wymagań dla audytorów wewnętrznych systemu zarządzania jakością zgodnego z normą PN-EN ISO 9001 lub wymagań równoważnych, tj. określonych na nie niższym poziomie jakości, potwierdzone ważnym certyfikatem dla audytora wewnętrznego systemu zarządzania jakością zgodnego z normą PN-EN ISO 9001 po zdaniu egzaminu;
g) minimum 2 osoby, które posiadają kwalifikacje potwierdzone ukończeniem studiów podyplomowych z zakresu ochrony danych osobowych oraz co najmniej 8-letnie doświadczenie zawodowe na stanowisku Inspektora Ochrony Danych lub Administratora Bezpieczeństwa Informacji;
h) minimum 2 osoby, które brały udział w realizacji co najmniej 2 projektów związanych z zarządzaniem ryzykiem w zakresie bezpieczeństwa informacji, w tym co najmniej 1 projekcie zrealizowanym zgodnie z normą ISO 27005 lub równoważną;
i) minimum 1 osoba posiadająca wiedzę oraz praktyczne umiejętności w zarządzaniu ryzykiem w obszarze ochrony informacji. Kwalifikacje tej osoby powinny być poświadczone ważnym certyfikatem lub równoważnym dokumentem ukończenia szkolenia w tym zakresie;
j) minimum 1 osoba, która posiada doświadczenie w prowadzeniu szkoleń i zrealizowała minimum 10 szkoleń dotyczących cyberbezpieczeństwa, bezpieczeństwa informacji lub ochrony danych, skierowanych do podmiotów publicznych;
k) minimum 1 osoba w zespole powinna posiadać wiedzę na temat wymagań określonych w Ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Kwalifikacje te muszą być potwierdzone ważnym certyfikatem lub równoważnym dokumentem ukończenia odpowiedniego szkolenia w tym zakresie;
l) minimum 1 osoba w zespole powinna posiadać wiedzę z zakresu zarządzania cyberbezpieczeństwem, potwierdzoną aktualnym certyfikatem lub równoważnym dokumentem ukończenia szkolenia w tym obszarze;
m) minimum 1 osoba, która ukończyła techniczne studia wyższe w dziedzinie cyberbezpieczeństwa i posiada tytuł inżyniera, co powinno być udokumentowane dyplomem ukończenia studiów wyższych;
n) minimum 1 osoba w zespole powinna posiadać specjalistyczną wiedzę i umiejętności w zakresie administrowania sieciami teleinformatycznymi, potwierdzone aktualnym certyfikatem lub równoważnym dokumentem ukończenia szkolenia w tym zakresie;
o) minimum 1 osoba powinna odbyć specjalistyczne szkolenie z zakresu cyberbezpieczeństwa, zgodnie z normami ISO 27001, 22301 oraz przepisami RODO. Wymagane jest potwierdzenie ukończenia szkolenia certyfikatem lub równoważnym dokumentem;

p) minimum 1 osoba posiadająca wiedzę i doświadczenie w zakresie zapewnienia cyberbezpieczeństwa infrastruktury Active Directory, potwierdzone ważnym certyfikatem lub równoważnym dokumentem ukończenia szkolenia w tym zakresie;
q) minimum 1 osoba posiadająca wiedzę i doświadczenie w zakresie białego wywiadu (OSINT) potwierdzone ważnym certyfikatem lub równoważnym dokumentem ukończenia szkolenia w tym zakresie;
r) minimum 1 osoba posiadająca wiedzę i doświadczenie w zakresie cyberbezpieczeństwa systemów OT, potwierdzone ważnym certyfikatem lub równoważnym dokumentem ukończenia szkolenia w tym zakresie;
s) minimum 1 osoba posiadająca wiedzę i doświadczenie w zakresie sztucznej inteligencji, potwierdzone ważnym certyfikatem lub równoważnym dokumentem ukończenia szkolenia w tym zakresie.

W celu potwierdzenia spełniania przez wykonawcę warunków udziału w postępowaniu dotyczących zdolności technicznej lub zawodowej, Zamawiający żąda następujących podmiotowych środków dowodowych:

a) referencje lub inny dokument potwierdzający prawidłowe wykonanie co najmniej 3 audytów bezpieczeństwa systemów teleinformatycznych, w tym co najmniej 1 z testami penetracyjnymi, na rzecz podmiotów realizujących zadania publiczne (niewskazanych w odpowiedzi na wymóg lit. b i c), z których każdy miał wartość nie mniejszą niż 50 000,00 zł brutto;
b) referencje lub inny dokument potwierdzający prawidłowe wykonanie 4 innych audytów cyberbezpieczeństwa (niewskazanych w odpowiedzi na wymóg lit. a i c) o wartości co najmniej 20 000,00 zł brutto w podmiotach realizujących zadania publiczne;
c) referencje lub inny dokument potwierdzający prawidłowe wykonanie co najmniej 15 innych audytów bezpieczeństwa informacji (niewskazanych w odpowiedzi na wymóg lit. a i b);
d) referencje lub inny dokument potwierdzający prawidłowe wykonanie co najmniej 2 usług przeprowadzenia szkoleń z zakresu cyberbezpieczeństwa dla podmiotów realizujących zadania publiczne, z których każda miała wartość nie mniejszą niż 20 000,00 zł brutto;
e) referencje lub inny dokument potwierdzający prawidłowe wykonanie co najmniej 5 projektów polegających na świadczeniu usług w zakresie opracowania dokumentacji systemu zarządzania bezpieczeństwem informacji dla podmiotów realizujących zadania publiczne;
f) referencje lub inny dokument potwierdzający prawidłowe wykonanie co najmniej 2 projektów dotyczących szacowania ryzyka dla bezpieczeństwa danych w systemach informatycznych, w tym w co najmniej 1 projekt dotyczący zarządzania ryzykiem na podstawie normy ISO 27005;
g) co najmniej 2 aktualne certyfikaty audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 lub równoważnej wydane przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób;

h) co najmniej 2 zaświadczenia ukończenia kursu Information Security Management Systems Auditor (ISMS);
i) certyfikat lub zaświadczenie ukończenia szkolenia w zakresie wdrożenia systemu zarządzania bezpieczeństwem informacji wg ISO 27001; lub równoważną,
j) certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301; lub równoważną,
k) certyfikat lub zaświadczenie ukończenia szkolenia w zakresie wdrażania systemu zarządzania ciągłością działania wg ISO 22301; lub równoważną,
l) co najmniej 2 certyfikaty audytora wewnętrznego systemu zarządzania jakością według normy PN-EN ISO 9001; lub równoważną,
m) co najmniej 2 dyplomy ukończenia studiów podyplomowych w zakresie ochrony danych osobowych i/lub bezpieczeństwa informacji;
n) referencje lub inne dokumenty potwierdzające co najmniej 8-letnie doświadczenie, co najmniej 2 osób, na stanowisku Inspektora Ochrony Danych/ Administratora Bezpieczeństwa Informacji;
o) certyfikat lub zaświadczenie ukończenia szkolenia w zakresie ryzyka w ochronie informacji;
p) referencje za przeprowadzenie co najmniej 10 szkoleń w zakresie bezpieczeństwa informacji;
q) certyfikat lub zaświadczenie ukończenia szkolenia w zakresie wymagań Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
r) certyfikat lub zaświadczenie ukończenia szkolenia w zakresie zarządzania cyberbezpieczeństwem;
s) dyplom ukończenia wyższych studiów technicznych w zakresie cyberbezpieczeństwa, potwierdzający uzyskanie tytułu inżyniera;
t) certyfikat lub zaświadczenie ukończenia szkolenia w zakresie administrowania sieciami teleinformatycznymi;
u) certyfikat lub zaświadczenie o odbyciu specjalistycznego szkolenia w zakresie cyberbezpieczeństwa na podstawie norm ISO 27001, 22301 lub równoważnych i przepisów RODO.
v) certyfikat lub zaświadczenie ukończenia szkolenia w zakresie zapewnienia cyberbezpieczeństwa infrastruktury Active Directory;
w) certyfikat lub zaświadczenie ukończenia szkolenia w zakresie białego wywiadu (OSINT);
x) certyfikat lub zaświadczenie ukończenia szkolenia w zakresie cyberbezpieczeństwa systemów OT;
y) certyfikat lub zaświadczenie ukończenia szkolenia w zakresie sztucznej inteligencji.

6. Termin i miejsce wykonania zamówienia

1. **Termin wykonania zamówienia:** Umowa zostanie wykonana w całości w terminie do **120** dni od dnia jej zawarcia. Za datę terminowego wykonania przedmiotu umowy uznaje się datę podpisania przez Zamawiającego końcowego protokołu odbioru bez zastrzeżeń.
2. **Miejsce wykonania zamówienia:** Siedziba Zamawiającego: Miejskie Przedsiębiorstwo Wodociągów i Kanalizacji Sp. z o.o. w Łasku, ul. Tylna 9, 98-100 Łask.

7. Miejsce, termin i sposób składania ofert

1. Ofertę należy złożyć wyłącznie w postaci elektronicznej, za pośrednictwem systemu teleinformatycznego **Baza Konkurencyjności (BK2021)**, poprzez wypełnienie formularza ofertowego i dodanie wymaganych załączników w ogłoszeniu dotyczącym niniejszego postępowania.
2. Termin składania ofert upływa w dniu: **07.05.2026 r.** o godzinie: **10:00.**
3. Oferty złożone po upływie wskazanego terminu lub w innej formie (np. e-mailem, papierowo) nie będą rozpatrywane.
4. Kompletna oferta składana w systemie powinna zawierać w szczególności:
    1. **Załącznik nr 2 – Formularz ofertowy** (zawierający m.in. całkowitą wartość oferty wyrażoną w kwocie netto i brutto, oświadczenie o braku powiązań kapitałowych i osobowych oraz oświadczenie o spełnieniu obowiązków informacyjnych RODO);
    2. **Załącznik nr 3 – Wykaz usług**;
    3. **Załącznik nr 4 – Wykaz osób**.

Do Wykazu usług oraz Wykazu osób należy dołączyć wymagane poświadczenia (referencje, certyfikaty). W przypadku ich braku, Zamawiający wezwie Wykonawcę do ich uzupełnienia w wyznaczonym terminie. Nieuzupełnienie dokumentów w wyznaczonym terminie skutkować będzie odrzuceniem oferty.

6. Opis sposobu obliczenia ceny

1. Cena oferty powinna obejmować **całkowity koszt wykonania przedmiotu zamówienia**, zgodnie z wymaganiami określonymi w dokumentacji postępowania, w szczególności:
- przeprowadzenie audytów bezpieczeństwa systemów teleinformatycznych,
- realizację testów penetracyjnych,
- opracowanie raportów z audytu,
- przygotowanie dokumentacji systemu zarządzania bezpieczeństwem informacji,
- realizację usług związanych z analizą i szacowaniem ryzyka,
- przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa,
- wszelkie inne czynności niezbędne do prawidłowego wykonania przedmiotu zamówienia.

2. Cena oferty powinna obejmować **wszystkie koszty związane z realizacją zamówienia**, w szczególności:
- koszty pracy zespołu ekspertów,
- koszty dojazdów i delegacji,
- koszty przygotowania raportów, dokumentacji oraz materiałów szkoleniowych,
- koszty narzędzi audytowych i testów penetracyjnych,
- koszty administracyjne oraz inne koszty pośrednie,
- należne podatki, w tym podatek VAT.

3. Wykonawca podaje cenę oferty jako:
    - **cenę netto**,
    - **kwotę podatku VAT**,
    - **cenę brutto**.
4. Cena oferty musi być wyrażona **w złotych polskich (PLN)**, z dokładnością do **dwóch miejsc po przecinku**.
5. Cena oferty ma charakter **ryczałtowy** i nie podlega zmianie w trakcie realizacji zamówienia, z wyjątkiem przypadków określonych w umowie.
6. W przypadku rozbieżności pomiędzy ceną podaną liczbą a słownie, za wiążącą uznaje się cenę podaną słownie.
7. Przy wyborze najkorzystniejszej oferty Zamawiający będzie kierował się kryterium: **Cena brutto – waga 100%**.
8. Punkty w kryterium ceny zostaną przyznane według następującego wzoru:
9. **C = (Cmin / Cbad) x 100 pkt**
10. gdzie:
    - **C** – liczba punktów przyznanych badanej ofercie
    - **Cmin** – najniższa cena brutto spośród wszystkich złożonych ofert (niepodlegających odrzuceniu)
    - **Cbad** – cena brutto oferty badanej

7. Klauzula informacyjna z art. 13 RODO

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO”, Zamawiający informuje, że:

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO”, Zamawiający informuje, że:

1. **Administrator Danych:** Administratorem danych osobowych Wykonawcy jest Miejskie Przedsiębiorstwo Wodociągów i Kanalizacji Sp. z o.o. w Łasku, ul. Tylna 9, 98-100 Łask.
2. **Inspektor Ochrony Danych (IOD):** W sprawach związanych z ochroną danych osobowych Wykonawca może kontaktować się z Inspektorem Ochrony Danych pod adresem e-mail: **[Wpisz adres e-mail IOD, np. iod@mpwiklask.pl]** lub listownie na adres siedziby Administratora.
3. **Cel i podstawa prawna przetwarzania:** Dane osobowe Wykonawcy będą przetwarzane na podstawie art. 6 ust. 1 lit. b oraz lit. c RODO w celu przeprowadzenia niniejszego postępowania o udzielenie zamówienia (wyłączonego spod rygorów ustawy Prawo zamówień publicznych,

realizowanego zgodnie z Zasadą Konkurencyjności), wyboru najkorzystniejszej oferty, zawarcia umowy oraz jej późniejszej realizacji, a także w celach związanych z audytem, rozliczeniem i kontrolą prawidłowości wydatkowania funduszy unijnych (KPO/FERC).

4. **Odbiorcy danych:** Odbiorcami danych osobowych Wykonawcy będą podmioty uprawnione do tego na podstawie powszechnie obowiązujących przepisów prawa, w tym instytucje nadzorujące i kontrolujące realizację projektów dofinansowanych ze środków UE (np. CPPC) oraz operator systemu Baza Konkurencyjności (BK2021). Dane mogą być również udostępniane na wniosek innych uczestników postępowania, z poszanowaniem zasad uczciwej konkurencji oraz ochrony tajemnicy przedsiębiorstwa.
5. **Okres przechowywania danych:** Dane osobowe Wykonawcy będą przechowywane przez okres trwania postępowania oraz realizacji umowy, a następnie przez czas wymagany do archiwizacji dokumentacji projektów dofinansowanych ze środków Unii Europejskiej (zgodnie z wytycznymi instytucji finansującej, nie krócej jednak niż przez okres 5 lat od dnia zakończenia projektu).
6. **Prawa osób, których dane dotyczą:** W odniesieniu do swoich danych osobowych Wykonawcy przysługuje:
    - prawo dostępu do swoich danych osobowych (na podstawie art. 15 RODO);
    - prawo do żądania ich sprostowania (na podstawie art. 16 RODO);
    - prawo do żądania ograniczenia przetwarzania (na podstawie art. 18 RODO), z zastrzeżeniem przypadków, w których przepisy prawa lub wytyczne unijne nie pozwalają na uwzględnienie żądania.
7. **Prawo wniesienia skargi:** Wykonawcy przysługuje prawo wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych (PUODO), gdy Wykonawca uzna, że przetwarzanie jego danych narusza przepisy RODO.
8. **Informacja o wymogu podania danych:** Podanie przez Wykonawcę danych osobowych jest dobrowolne, jednakże jest warunkiem niezbędnym do wzięcia udziału w niniejszym postępowaniu. Konsekwencją niepodania danych będzie odrzucenie oferty lub brak możliwości zawarcia umowy.
9. **Zautomatyzowane podejmowanie decyzji:** Dane osobowe Wykonawcy nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

8. Informacje dodatkowe i postanowienia końcowe

1. Zamawiający zastrzega sobie prawo do wzywania Wykonawców do złożenia dodatkowych wyjaśnień dotyczących treści złożonych ofert, a także wzywania do uzupełnienia drobnych braków formalnych w dokumentacji (np. brakujących referencji czy zaświadczeń) w wyznaczonym terminie. Niedopuszczalne jest jednak wprowadzanie jakichkolwiek istotnych zmian w treści samej oferty, w tym w oferowanej cenie (z zastrzeżeniem ust. 2).
2. W przypadku gdy cena najkorzystniejszej oferty przekracza budżet, jaki Zamawiający zamierzał przeznaczyć na sfinansowanie zamówienia, Zamawiający zastrzega sobie prawo do podjęcia negocjacji cenowych z Wykonawcą (lub Wykonawcami). Negocjacje nie mogą prowadzić do zmiany zakresu przedmiotu zamówienia ani pierwotnych warunków realizacji umowy.

3. Zamawiający zastrzega sobie prawo do zamknięcia postępowania bez wyboru najkorzystniejszej oferty lub unieważnienia postępowania na każdym jego etapie, w szczególności w przypadku gdy:
    - cena najkorzystniejszej oferty przewyższa kwotę, którą Zamawiający zamierza przeznaczyć na sfinansowanie zamówienia (a negocjacje nie przyniosły rezultatu);
    - wystąpiła istotna zmiana okoliczności powodująca, że prowadzenie postępowania lub wykonanie zamówienia nie leży w interesie Zamawiającego lub interesie publicznym;
    - środki publiczne (w tym środki z funduszy UE), które Zamawiający zamierzał przeznaczyć na sfinansowanie całości lub części zamówienia, nie zostały mu ostatecznie przyznane;
    - postępowanie obarczone jest niemożliwą do usunięcia wadą.
4. W przypadku unieważnienia postępowania Wykonawcom nie przysługuje żadne roszczenie o zwrot kosztów przygotowania ofert.

9. Załączniki do zapytania ofertowego:

Załącznik nr 1 – Formularz ofertowy
Załącznik nr 2 – Projekt Umowy
Załącznik nr 3 – Wykaz usług (doświadczenie Wykonawcy)
Załącznik nr 4 – Wykaz osób skierowanych do realizacji zamówienia

Z poważaniem

Elektronicznie
podpisany przez
Mariusz Sowiński
Data: 2026.04.30
14:41:49 +02'00'

.....

Miejskie Przedsiębiorstwo Wodociągów i Kanalizacji
Sp. z o.o. w Łasku