**Załącznik nr: 1**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Przedmiotem zamówienia jest wdrożenie systemu zarządzania bezpieczeństwem informacji zgodnego z normą ISO/IEC 27001:2013 (PN-EN ISO/IEC 27001:2017).**

**A/** **Przedmiot zamówienia obejmuje następujące działania:**

1. Prace szkoleniowe, konsultacyjne, weryfikacyjne oraz działania polegające na opracowaniu niezbędnej dokumentacji systemu zarządzania bezpieczeństwem informacji zgodnego z wymaganiami normy ISO/IEC 27001
2. Prace szkoleniowe, konsultacyjne, weryfikacyjne oraz działania polegające na opracowaniu niezbędnej dokumentacji lub wprowadzeniu zmian do już funkcjonującej w zakresie systemu zarządzania jakością oraz zarządzania środowiskowego
3. Integracje systemu zarządzania bezpieczeństwem informacji z funkcjonującym i zaktualizowanym systemem zarządzania jakością i systemem zarządzania środowiskowego

**B/ Celem zamówienia jest:**

1. Wdrożenie skutecznego systemu zarządzania bezpieczeństwem informacji zgodnego z wymaganiami normy ISO/IEC 27001 potwierdzonego przyznanym Zamawiającemu stosownym certyfikatem, uzyskanym w systemie akredytacji, w wyniku audytu niezależnej jednostki certyfikującej.
2. Aktualizacja obecnie funkcjonującego systemu zarządzania jakością oraz zarządzania środowiskowego i zapewnienie jego zgodności z wymaganiami norm ISO 9001:2015 oraz ISO 14001:2015, potwierdzonymi przyznanymi Zamawiającemu stosownymi certyfikatami uzyskanymi w systemie akredytacji w wyniku audytu niezależnej jednostki certyfikującej.
3. Zapewnienie odpowiedniej efektywności systemu zarządzania w poszczególnych obszarach poprzez integrację powiązanych regulacji.

**C/ W ramach realizacji przedmiotu zamówienia Zamawiający wymaga realizacji niżej określonych zadań:**

1. **Etap I: SZKOLENIA WSTĘPNE**
   1. Przeprowadzenie szkoleń dla kadry zarządzającej oraz zespołu wdrożeniowego (około 20 osób) w siedzibie Zamawiającego w formie wykładu wraz z ćwiczeniami z zakresu:
      1. zasad bezpieczeństwa informacji zgodnie z wymogami normy ISO/IEC 27001:2013
      2. Wskazanie podobieństw i różnic pomiędzy normami ISO 9001:2008 i ISO 14001:2004 normami wydanymi w 2015 r.
   2. Przeprowadzenie w siedzibie Zamawiającego w formie wykładu wraz z ćwiczeniami szkolenia dla audytorów wewnętrznych (16 osób ) systemu zarządzania bezpieczeństwem informacji zgodnego z normą ISO/IEC 27001:2013, systemu zarzadzania jakością zgodnego z normą ISO 9001:2015 oraz systemu zarządzania środowiskowego zgodnego z normą ISO 14001:2015. Zakres szkolenia powinien obejmować zarówno interpretację wymagań norm, jak również zagadnienia z zakresu planowania, realizacji i dokumentowania wyników audytów wewnętrznych.
2. **Etap II: AUDYT WSTĘPNY Z ZAKRESU BEZPIECZEŃSTWA INFORMACJI („Zerowy”)**
   1. Analizę i przegląd dokumentacji i zapisów powiązanych z bezpieczeństwem informacji pod kątem zgodności z wymaganiami normy ISO /IEC 27001 oraz mających zastosowanie przepisów prawa w szczególności przepisów prawa o ochronie danych osobowych
   2. Wizję lokalną w każdej z lokalizacji, w której prowadzona jest działalność w celu oceny stosowalności obecnych regulacji.
   3. Określenie stanu faktycznego wszystkich stosowanych zabezpieczeń w zakresie bezpieczeństwa informacji (audyt zgodności i skuteczności zabezpieczeń zgodnych z wymaganiami załącznika A normy ISO/IEC 27001:2013)
   4. Dokumentowanie wyników audytu wewnętrznego wraz z wykazem rozbieżności oraz adekwatnych działań naprawczych
3. **Etap II: AUDYT WSTĘPNY Z ZAKRESU ZARZĄDZANIA JAKOŚCIĄ I ZARZĄDZANIA ŚRODOWISKOWEGO („Inwentaryzacja stanu obecnego”)**
   1. Kompleksowy przegląd obecnej dokumentacji systemowej pod kątem zmian jakie należy wprowadzić w celu zapewnienia zgodności z wymaganiami normy ISO 9001:2015 oraz ISO 14001:2015
   2. Przeprowadzenie identyfikacji mających zastosowanie przepisów prawa i innych wymagań z zakresu ochrony środowiska do których spełnienia organizacja jest zobowiązana oraz przeprowadzenie oceny zgodności z tymi wymaganiami
   3. Opracowanie raportu zawierającego zdefiniowany zakres zmian jakie należy wprowadzić do systemu, koncepcję wprowadzania tych zmian oraz sposobu ich wdrożenia
   4. Opracowanie raportu z oceny zgodności z przepisami prawa i innymi wymaganiami z zakresu ochrony środowiska wraz ze wskazaniem rozbieżności oraz działań naprawczych
4. **Etap IV: INWENTARYZACJA AKTYWÓW I ICH PODATNOŚCI ORAZ SZACOWANIE RYZYKA W SZBI**
   1. Określenie szczegółowego zakresu systemu zarządzania bezpieczeństwem informacji
   2. Określenie odpowiedzialności i uprawnień w systemie bezpieczeństwa informacji:
      1. Aktualizacja schematu organizacyjnego
      2. Powołanie i zdefiniowanie zakresu odpowiedzialności i uprawnień dla Pełnomocnika ds. SZBI
      3. Powołanie Zespołu ds. Szacowania Ryzyka oraz określenie zakresu odpowiedzialności i uprawnień dla członków zespołu.
   3. Wybór odpowiedniej dla organizacji metody oceny ryzyka
   4. Przeprowadzenie szkolenia dla Zespołu ds. Szacowania Ryzyka z metody inwentaryzacji i klasyfikacji aktywów informacyjnych, z wybranej metody oceny ryzyka w bezpieczeństwie informacji oraz strategii i planów postępowania z ryzykiem
   5. Wsparcie dla organizacji w zakresie inwentaryzacji i klasyfikacji aktywów informacyjnych oraz określenia ich podatności.
   6. Wsparcie dla Zespołu ds. Oceny Ryzyka w zakresie szacowania ryzyka, nadzorowanie prac zespołu oraz weryfikacja uzyskanych, udokumentowanych wyników.
   7. Określenie we współpracy z Zespołem ds. Oceny Ryzyka oraz funkcjami zainteresowanymi strategii postępowania z ryzykiem oraz planów postępowania z ryzykiem w tym:
      1. Zdefiniowanie zabezpieczeń i celów ich stosowania
      2. Udokumentowanie Deklaracji Stosowania
      3. Określenie celów i zadań dla systemu zarzadzania bezpieczeństwem informacji

**UWAGA do etapu IV**

W przypadku stwierdzenia przez audytorów instytucji certyfikującej małych lub średnich niezgodności, Wykonawca zobowiązuje się do podjęcia wspólnie z pracownikami czynności naprawczych celem uzyskania pozytywnej oceny z audytu, a tym samym „pozytywnego sprawozdania” z realizacji IV etapu.

1. **Etap V: OKREŚLENIE KONTEKSTU ORGANIZACJI ORAZ OCENA RYZYKA W ODNIESIENIU DO JAKOŚCI I ZARZĄDZANIA ŚRODOWISKOWEGO**
   1. Określenie stron zainteresowanych oraz ich wymagań względem organizacji (Zamawiającego) w szczególności względem jakości i zarządzania środowiskowego
   2. Określenie czynników wewnętrznych i zewnętrznych mających lub mogących mieć wpływ na jakość lub środowisko, w szczególności na zgodność i skuteczność systemów zarządzania
   3. Powołanie Zespołu ds. Szacowania Ryzyka w systemie zarządzania jakością i zarządzania środowiskowego oraz określenie zakresu odpowiedzialności i uprawnień dla członków zespołu.
   4. Wybór odpowiedniej dla organizacji metody oceny ryzyka
   5. Przeprowadzenie szkolenia dla Zespołu ds. Szacowania Ryzyka z wybranej metody oceny ryzyka w systemie jakościowym i środowiskowym oraz określania strategii i planów postępowania z ryzykiem
   6. Wsparcie dla Zespołu ds. Oceny Ryzyka w zakresie szacowania ryzyka, nadzorowanie prac zespołu oraz weryfikacja uzyskanych, udokumentowanych wyników.
   7. Określenie we współpracy z Zespołem ds. Oceny Ryzyka oraz stronami zainteresowanymi strategii postępowania z ryzykiem oraz planów postępowania z ryzykiem w tym:
      1. Zdefiniowanie zabezpieczeń infrastrukturalnych oraz proceduralnych
      2. Określenie wdrożenia tych zabezpieczeń do systemu zarządzania jakością i zarządzania środowiskowego.
2. **Etap VI: OPRACOWANIE NIEZBĘDNEJ DOKUMENTACJI SYSTEMOWEJ** 
   1. Opracowanie wspólnie z pracownikami zamawiającego wymaganych dokumentów systemowych z zakresu bezpieczeństwa informacji:
      1. Opracowanie Polityki Systemu Zarządzania Bezpieczeństwem Informacji;
      2. Opracowanie dokumentacji wynikającej z Rozporządzenia o Ochronie Danych Osobowych (RODO)
      3. Opracowanie procedur systemowych (aktualizacja obecnie funkcjonujących w ramach systemu jakościowego i środowiskowego) w szczególności w zakresie:
         1. Audytu wewnętrznego
         2. Działań naprawczych i korygujących
         3. Zarządzania ryzykiem
         4. Nadzoru nad udokumentowanymi informacjami
      4. Opracowanie Instrukcji postępowania na wypadek wykrycia incydentu naruszenia bezpieczeństwa
      5. Opracowanie planów ciągłości działania
      6. Opracowanie pozostałych procedur i instrukcji wymaganych przez normę ISO/IEC 27001 oraz wynikających z oceny ryzyka
   2. Aktualizacja wspólnie z pracownikami zamawiającego dokumentacji systemu zarządzania jakością oraz zarządzania środowiskowego w celu zapewnienia jej zgodności z wymaganiami ISO 9001:2015 oraz ISO 14001:2015 oraz adekwatności do uzyskanych wyników oceny ryzyka.
   3. Integracja dokumentacji systemu zarządzania bezpieczeństwem informacji oraz systemu zarządzania jakością i zarządzania środowiskowego.
   4. Przeprowadzenie szkoleń dla kadry zarządzającej z zakresu nowych regulacji i ich stosowania

szkolenie dla 4 grup (w sumie ok 70 os.)

* 1. Opracowanie programu uświadamiania i szkolenia personelu organizacji. Przygotowanie prezentacji oraz broszury informacyjnej na potrzeby przeprowadzenia szkolenia pracowników

1. **Etap VII: WDRAŻANIE TECHNICZNYCH I ORGANIZACYJNYCH ZABEZPIECZEŃ**
   1. Konsultacje przy wdrożeniu zabezpieczeń w infrastrukturze systemu informatycznego;
   2. Współpraca oraz konsultacje z podwykonawcami podczas projektowania aplikacji do obsługi danych medycznych w zakresie tworzenia mechanizmów zapewnienia bezpieczeństwa przechowywania i przetwarzania danych;
   3. Konsultacje przy wdrożeniu zabezpieczeń organizacyjnych – polityki bezpieczeństwa danych osobowych, zapisów w umowach z dostawcami, procedur itp.
   4. Konsultacje przy wdrażaniu zabezpieczeń proceduralnych
   5. Konsultacje w zakresie ćwiczeń i testowania skuteczności zabezpieczeń
2. **Etap VIII: AUDYT WERYFIKACYJNY I MONITOROWANIE ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA** 
   1. Przeprowadzenie audytów wewnętrznych całego systemu zarządzania jakością, zarządzania środowiskowego oraz zarządzania bezpieczeństwem informacji we wszystkich lokalizacjach wraz z audytorami wewnętrznymi Zamawiającego (w roi audytorów trenujących)
      1. Weryfikacja zgodności z wymaganiami przedmiotowych norm (ISO/IEC 27001:2013, ISO 9001:2015, ISO 14001:2015) oraz regulacji wewnętrznych
      2. Dokumentowanie wyników audytów wewnętrznych zgodnie z obowiązującą procedurą systemową Zamawiającego
      3. Planowanie działań naprawczych oraz korygujących
   2. Przeprowadzenie wraz z pracownikami Zamawiającego przeglądu zintegrowanego systemu zarządzania jakością, zarządzania środowiskowego oraz zarządzania bezpieczeństwem informacji w zakresie wynikającym z przedmiotowych norm
      1. Pomoc w zebraniu danych wejściowych
      2. Moderowanie przeglądu zarządzania przez kierownictwo
      3. Dokumentowanie wyników – opracowanie raportu z przeglądu zarządzania wraz z wykazem działań do realizacji (naprawcze, korygujące i doskonalące)
3. **Etap IX: OBECNOŚĆ I WSPARCIE W TRAKCIE AUDYTU ZEWNĘTRZNEGO REALIZOWANEGO PRZEZ NIEZALEŻNĄ, AKREDYTOWANĄ JEDNOSTKĘ CERTYFIKUJĄCĄ**
   1. Obecność w trakcie trwania audytu zewnętrznego (obie fazy audytu)
   2. Zaplanowanie działań odnoszących się do wyników audytu
   3. Wprowadzenie niezbędnych zmian do dokumentacji systemowej w przypadku jeśli wdrożenie działań odnoszących się do obserwacji audytowych będą tego wymagały.

**Załącznik nr:2**

**WYMAGANIA ZAMAWIAJĄCEGO**

1. Realizacja projektu nie może być zlecona podmiotom trzecim.

2. W ramach realizacji przedmiotu umowy, Wykonawca musi zapewnić dostępność konsultantów w siedzibie Zamawiającego w wymiarze min. 30 dni roboczych, max.60 dni roboczych.

3. Cena oferty musi obejmować wszystkie koszty związane z wykonaniem przedmiotu umowy w szczególności koszty materiałów szkoleniowych oraz wszystkich innych opracowań, koszty dojazdów i pobytu konsultantów w siedzibie Zamawiającego oraz wszystkie pozostałe koszty, które będzie ponosił Zamawiający.

1. Każdy Wykonawca może złożyć tylko jedną ofertę. Zamawiający nie dopuszcza składania ofert wariantowych.

5. Każdy Wykonawca składający ofertę musi spełniać poniższe wymagania:  
1) zapewnić personel o kompetencjach umożliwiających realizację projektu:

a) Wykonawca musi zagwarantować minimum jednego konsultanta do każdego z przedmiotowych systemów ISO 9001:2015; ISO14001:2015),

b) konsultanci muszą posiadać udokumentowane szkolenia uprawniające do pełnienia funkcji audytorów wiodących przedmiotowych systemów,

c) w zespole konsultantów musi znajdować się co najmniej 1 osoba z wykształceniem wyższym informatycznym, z minimum 3 letnim doświadczeniem, posiadająca uprawnienia audytora normy ISO 27001.

2) posiadać doświadczenie w realizacji przedmiotu zamówienia:

a) we wdrażaniu normy ISO 27001 w min. 1 placówce ochrony zdrowia ochrony zdrowia ( w szpitalu) zatrudniających min.500 osób

b) we wdrażaniu normy ISO 27001 w ochronie zdrowia w min.10 jednostkach

c) realizacja projektów wdrożeniowych lub dostosowawczych w min. 20 jednostkach.

**Uwaga: Wymagania określone w pkt.5 należy potwierdzić odpowiednimi dokumentami:**

**ppkt.1) certyfikaty, zaświadczenia;**

**ppkt.2) referencje.**

6. **Umowa zostanie zawarta na okres od dnia zawarcia umowy do 30.06.2018 roku.**

7. Kryteria oceny oferty: Cena – 60 %;

Dostępność konsultantów w siedzibie Zamawiającego – 40 %

Kryteria oceny zostaną obliczone wg. Poniższego wzoru

|  |
| --- |
| **Cena – C** maksymalna liczba punktów do zdobycia w tym kryterium –60.  **C = ( Cmin/Cof ) x 60**  gdzie: **C-**  razem ilość punktów uzyskana przez ofertę badaną  - Cmin - najniższa cena spośród wszystkich ofert  - Cof - cena oferty badanej |

**Dostępność konsultantów w siedzibie Zamawiającego – D** maksymalna liczba punktów do zdobycia w tym kryterium – 40

Zamawiający wymaga nin.30 dni roboczych- max.60 dni roboczych.

**D= (Dof/Dmax) x 40**

gdzie: D - razem ilość punktów uzyskana przez ofertę badaną

- Dof – ilość dni z oferty badanej

- Jmax – maksymalna ilość dni spośród wszystkich ofert

Za najkorzystniejszą zostanie uznana oferta, która uzyska najwyższą ilość punktów obliczoną na podstawie ustalonych kryteriów:

**R= C+D**

Gdzie: R – razem ilość punktów uzyskana przez ofertę badaną

C- ilość punktów uzyskana za cenę

D- ilość punktów uzyskana za dostępność

Obliczenia będą dokonywane do dwóch miejsc po przecinku

8.Oferta musi zawierać:

* + - 1. Formularz cenowy
      2. Wstępny harmonogram wdrożenia systemu zarządzania bezpieczeństwem informacji przygotowany na podstawie zadań określonych w pkt. C ( Załącznika nr:1) – poszczególnych etapów wdrażania systemu.
      3. Oświadczenie podpisane przez Wykonawcę ( Zał nr. 3).
      4. Zaakceptowany wzór umowy ( Zał nr:4)