Załącznik nr 1
do zapytania
ofertowego/umowy

Opis Przedmiotu Zamówienia
(zwany ,,OPZ")

I. Ogólne warunki realizacji zamówienia

1. Przedmiotem zamówienia jest opracowanie przez Wykonawcę dla Zamawiającego systemu zarządzania bezpieczeństwem informacji, zwanego ,,SZBI", przeprowadzenie szkoleń, zwanych ,,Szkoleniami" wraz z przekazaniem materiałów szkoleniowych oraz świadczenie usług asysty wdrożeniowej, zwanych ,,Usługami asysty", zgodnie z Umową, zwane ,,Przedmiotem Umowy".
2. Przedmiot Umowy będzie realizowany w pięciu etapach:
   1) Etap I – przeprowadzenie szkolenia z zakresu bezpieczeństwa informacji oraz systemów zarządzania dla kierownictwa RDOŚ, pełnomocnika bezpieczeństwa informacji i administratora systemów bezpieczeństwa informacji;
   2) Etap II - analiza działalności Zamawiającego i sporządzenie Sprawozdania;
   3) Etap III - opracowanie SZBI;
   4) Etap IV - przeprowadzenie Szkolenia i przekazanie materiałów szkoleniowych;
   5) Etap V - świadczenie Usług asysty,

   zwanych dalej „Etapami", które szczegółowo określa niniejszy OPZ.
3. Wykonawca zobowiązuje się wykonać Przedmiot Umowy w terminach określonych w Umowie.

II. ETAP I

W ramach Etapu I Wykonawca:

1) przeprowadzi szkolenie z zakresu bezpieczeństwa informacji oraz systemów zarządzania uwzględniającego w programie następującą tematykę:
   a) Wprowadzenie
      - Pojęcia związane z bezpieczeństwem informacji,
      - Zarządzanie Bezpieczeństwem Informacji w organizacji, na podstawie obowiązujących przepisów prawa,
      - Źródła wymagań i zaleceń – norma ISO 27001 oraz ISO 27002.
   b) Planowanie i wdrożenie systemu zarządzania
      - Zasady wdrożenia systemu zarządzania bezpieczeństwem informacji,
      - Podział ról, zakresów obowiązków oraz odpowiedzialności za system w organizacji,
      - Analiza ryzyka bezpieczeństwa informacji,
      - Zarządzanie ryzykiem bezpieczeństwa informacji,
      - Zabezpieczenia techniczne i organizacyjne,
      - Struktura dokumentacji systemu zarządzania,
      - Szkolenia pracowników.
   c) Utrzymanie systemu zarządzania,
      - Przegląd systemu zarządzania,
      - Doskonalenie systemu zarządzania.
2) Czas trwania szkolenia – minimum 5 godzin, w tym 2 przerwy 15-minutowe. Preferowane godziny szkolenia 9.00 – 14.00,
3) Forma organizacji szkolenia – stacjonarne,
4) Wykonawca udostępni uczestnikom szkolenia materiały szkoleniowe.

5) Uczestnicy szkolenia będą mieli możliwość zadawania pytań w trakcie lub po omówieniu tematyki szkolenia.
6) Wykonawca udostępni uczestnikom szkolenia materiały szkoleniowe.
7) Wykonawca wystawi zaświadczenia o ukończeniu szkolenia dla pracowników RDOŚ.
8) Wykonawca wystawi odrębną fakturę za przeprowadzenie szkolenia, uwzględniającą zwolnienie z podatku VAT.

III. ETAP II

1. W ramach Etapu II wykonawca:
   1) przeprowadzi analizę zwaną dalej „Analizą", której celem jest identyfikacja kontekstu SZBI u Zamawiającego, obejmującą w szczególności:
      a) obszary działalności Zamawiającego i realizowanych zadań,
      b) strukturę organizacyjną Zamawiającego,
      c) specyfikę pracy poszczególnych komórek organizacyjnych Zamawiającego,
      d) systemy informatyczne użytkowane przez Zamawiającego,
      e) rejestry publiczne pozostające we właściwości Zamawiającego,
      f) wstępną identyfikację informacji przetwarzanych u Zamawiającego,
      g) wstępną identyfikację ryzyk związanych z utratą poufności, integralności i dostępności informacji przetwarzanych u Zamawiającego - w ramach której Wykonawca dokona oceny ryzyk i szans niezbędnych do zaprojektowania SZBI – również poprzez weryfikację działalności Zamawiającego m.in. w jego siedzibie oraz 3 placówkach zamiejscowych w Elblągu, Ełku i Jeleniu (konieczność przeprowadzenia wizji lokalnej).
   2) sporządzi sprawozdanie, zwane dalej ,,Sprawozdaniem":
      a) podsumowujące przeprowadzoną Analizę w zakresie, o którym mowa w ust.1 pkt 1,
      b) obejmujące propozycje rozwiązań i zmian w zakresie bezpiecznego przetwarzania informacji u Zamawiającego i wprowadzenia SZBI,
      c) obejmujące wstępną koncepcję SZBI, dostosowaną do potrzeb Zamawiającego, w tym do ryzyk właściwych dla Zamawiającego, zidentyfikowanych w wyniku Analizy, w szczególności wskazującą na główne obszary i rodzaje procedur, które powinny zostać uregulowane w SZBI.
2. W celu przeprowadzenia Analizy Zamawiający udostępni Wykonawcy niezbędne, posiadane dokumenty.
3. Sprawozdanie zostanie przekazane Zamawiającemu w formie edytowalnego pliku elektronicznego (doc lub docx) oraz w formie elektronicznej (opatrzonej kwalifikowanym podpisem elektronicznym).
4. Celem opracowania przez Wykonawcę wstępnej koncepcji SZBI, Zamawiający wskazuje poniżej ogólny ramowy zarys SZBI: Określenie struktury dokumentacji SZBI, która powinna mieć układ hierarchiczny, tj. opisywać SZBI na różnych poziomach szczegółowości oraz określać zagadnienia, które muszą zostać obligatoryjnie uregulowane:
   1) poziom jednostki (Zamawiający) - nadrzędny dokument ,,Polityka Bezpieczeństwa Informacji" Zamawiającego, który określa wymagania i zasady bezpieczeństwa informacji obowiązujące u Zamawiającego oraz sposób organizacji SZBI - z tym dokumentem powinny być spójne pozostałe dokumenty w SZBI,
   2) poziom systemów teleinformatycznych - polityka bezpieczeństwa systemów teleinformatycznych, na które składają się :
      – dokument ,,Polityka Bezpieczeństwa Systemów Teleinformatycznych", który opisuje wymagania i zasady bezpieczeństwa dla systemów teleinformatycznych,
      – odniesienia co do wymagań dotyczących zakresu dokumentacji poszczególnych systemów teleinformatycznych - np. dokumenty: polityki bezpieczeństwa poszczególnych systemów teleinformatycznych, które opisują w jaki sposób zasady i wymagania bezpieczeństwa zawarte w ,,Polityce Bezpieczeństwa Informacji" i ,,Polityce Bezpieczeństwa Systemów Teleinformatycznych" są realizowane w danym systemie teleinformatycznym,
   3) poziom procedur, instrukcji i regulaminów – procedury, instrukcje, regulaminy i inne dokumenty SZBI tworzone w celu uszczegółowienia zasad opisanych

w ww. politykach, dotyczące w szczególności zagadnień:

- bezpieczeństwo zasobów ludzkich,
- bezpieczeństwo fizyczne,
- bezpieczeństwo cyberprzestrzeni,
- bezpieczeństwo danych osobowych,
- bezpieczeństwo informacji niejawnych,
- obsługa incydentów,
- zarządzanie ryzykiem,
- użytkowanie systemów teleinformatycznych w RDOŚ w Olsztynie,
- użytkowanie urządzeń mobilnych.

5. Ramowy zarys SZBI, o którym mowa w ust. 4, nie ma charakteru bezwzględnie wiążącego i stanowi jedynie propozycję Zamawiającego. W przypadku nieuwzględnienia przez Wykonawcę wstępnej koncepcji SZBI ramowego zarysu lub jego poszczególnych elementów, Wykonawca uzasadni powyższe Zamawiającemu.

IV. ETAP III

1. W ramach Etapu III Wykonawca, na podstawie wyników Analizy i zaakceptowanego przez Zamawiającego Sprawozdania, opracuje SZBI, dostosowany do potrzeb Zamawiającego.
2. SZBI, który opracuje Wykonawca, stanowić będzie system zarządzania bezpieczeństwem informacji w RDOŚ w Olsztynie.
3. SZBI powinien być zgodny z przepisami ustawy z dnia 17 lutego 2005 r. o *informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz. U. z 2024 r. poz. 307, z późn. zm.), aktami wykonawczymi do ww. ustawy, wymaganiami normy PN-ISO/IEC 27001, w tym obejmować czternaście następujących obszarów mających wpływ na bezpieczeństwo w organizacji Zamawiającego:
   1) Polityka Bezpieczeństwa;
   2) Organizacja bezpieczeństwa informacji;
   3) Bezpieczeństwo zasobów ludzkich;
   4) Zarządzanie aktywami;
   5) Kontrola dostępu;
   6) Kryptografia;
   7) Bezpieczeństwo fizyczne i środowiskowe;
   8) Bezpieczna eksploatacja;
   9) Bezpieczna komunikacja;
   10) Pozyskiwanie, rozwój i utrzymanie systemów;
   11) Relacje z dostawcami;
   12) Zarządzanie incydentami związanymi z bezpieczeństwem informacji;
   13) Aspekty bezpieczeństwa w zarządzaniu ciągłością działania;
   14) Zgodność z wymaganiami prawnymi i własnymi standardami.

   Ponadto, SZBI powinien uwzględniać wymagania norm: PN-ISO/IEC 27002, PN-ISO/IEC 27005 oraz PN-ISO/IEC 24762.
4. SZBI musi być zgodny z aktualnymi przepisami powszechnie obowiązującego prawa, w szczególności z przepisami:
   1) 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);
   2) ustawy z dnia 10 maja 2018 r. o *ochronie danych osobowych;*

3) ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne;*
4) ustawy z dnia 6 września 2001 r. *o dostępie do informacji publicznej;*
5) ustawy z dnia 3 października 2008 r. o *udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowiska;*
6) ustawy z dnia 5 sierpnia 2010 r. o *ochronie informacji niejawnych;*
7) ustawy z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa;*
8) Rozporządzenia Rady Ministrów z dnia 21 maja 2024r. w sprawie Krajowych Ram Interoperacyjności minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych
9) Dyrektywy 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.

5. W ramach opracowania SZBI Wykonawca między innymi:
   1) zaproponuje obszary funkcjonalne, które powinny zostać objęte SZBI, spójne z treścią Sprawozdania zaakceptowanego przez Zamawiającego;
   2) uwzględnienie w szczególności następujących zagadnień:
      a) określenie organizacji bezpieczeństwa informacji,
      b) identyfikacja aktywów informacyjnych i klasyfikacji informacji przetwarzanych u Zamawiającego,
      c) szacowanie ryzyka oraz postępowania z ryzykiem, związanych z utratą poufności, integralności i dostępności informacji przetwarzanych u Zamawiającego,
      d) bezpieczeństwo w procesach zarządzania zasobami ludzkimi,
      e) szkolenia z zakresu bezpieczeństwa informacji,
      f) kontrola dostępu,
      g) bezpieczeństwo fizyczne i środowiskowe,
      h) klasyfikacja informacji,
      i) odpowiedzialność za zasoby,
      j) postępowanie z nośnikami informacji,
      k) użytkowanie urządzeń mobilnych i praca zdalna,
      l) zarządzanie sprzętem informatycznym,
      m) instalacja oprogramowania,
      n) ochrona przed oprogramowaniem złośliwym,
      o) kopie zapasowe,
      p) zarządzanie zmianami, w szczególności w systemach informatycznych oraz infrastrukturze informatycznej,
      q) zarządzanie dokumentacją infrastruktury informatycznej,
      r) monitorowanie systemów informatycznych,
      s) zarządzanie pojemnością systemów,
      t) serwis i konserwacja infrastruktury informatycznej,
      u) zarządzanie podatnościami technicznymi,
      v) zarządzanie incydentami bezpieczeństwa,
      w) zabezpieczenia kryptograficzne,
      x) bezpieczeństwo sieci i transmisji danych,
      y) ochrona własności intelektualnej,
      z) bezpieczeństwo informacji w relacjach z dostawcami,
      aa) ciągłość działania,
      bb) zasady bezpieczeństwa informacji w procesach pozyskiwania, rozwoju i utrzymania systemów informacyjnych,
      cc) weryfikacja zgodności z wymaganiami prawnymi,
      dd) korzystanie z poczty elektronicznej i Internetu,
      ee) zarządzanie usługami informatycznymi,
      ff) utrzymanie i doskonalenie SZBI,
      gg) przeprowadzanie audytów SZBI.

6. Wykonawca wraz z SZBI przedstawi zestawienie, zwane ,,Zestawieniem, w którym wykaże spełnienie przez SZBI wymagań dotyczących bezpieczeństwa informacji wynikających z aktualnych przepisów powszechnie obowiązującego prawa, a także odpowiednich norm.
7. SZBI oraz Zestawienie zostaną przekazane Zamawiającemu w formie edytowalnego pliku elektronicznego (doc lub .docx) oraz w formie elektronicznej (opatrzonej kwalifikowanym podpisem elektronicznym).
8. Zamawiający zastrzega sobie prawo do każdorazowego wnoszenia uwag do zaproponowanego przez Wykonawcę SZBI, w tym do rodzaju dokumentów, ich liczby, nazewnictwa, zakresu merytorycznego. Uwagi Zamawiającego powinny być każdorazowo uwzględnione przez Wykonawcę. W przypadku, gdyby proponowane przez Zamawiającego zmiany mogły powodować niezgodność dokumentacji z Umową, Wykonawca poinformuje o tym wcześniej Zamawiającego, uzasadniając swoje stanowisko - w takim przypadku Zamawiający podejmie ostateczną decyzję w zakresie konieczności uwzględnienia jego uwag przez Wykonawcę .

V. ETAP IV

1. W ramach Etapu IV Wykonawca:
   1) przeprowadzi szkolenie (trwające min. 4h) dla osób odpowiedzialnych u Zamawiającego za funkcjonowanie SZBI (maksymalnie 4 osób) obejmujące w szczególności:
      a) omówienie podstawowych zasad bezpieczeństwa informacji i wypełniania procedur, wynikających z SZBI,
      b) zagrożenia związane z przetwarzaniem informacji u Zamawiającego,
      c) zapoznanie z nowym SZBI, w szczeg6lnosci poprzez przedstawienie Zamawiającemu głównych obszarów, poszczególnych ścieżek procedur i zasad reagowania na incydenty, wynikających z SZBI,
      d) odpowiedzialność za naruszenie zasad związanych z SZBI;
   2) przygotuje materiały szkoleniowe w formie edytowalnego pliku elektronicznego (doc lub .docx), wskazujące na istotę funkcjonowania SZBI, uwzględniające główne obszary SZBI i wynikające z nich procedury, zaprezentowane w sposób syntetyczny i przejrzysty (np. ilustracje, schematy, tabele), dostosowane do potrzeb Zamawiającego. Materiały te zostaną udostępnione pracownikom Zamawiającego (np. w ramach wewnętrznej sieci Intranet) celem zapoznania ich z problematyką związaną z bezpieczeństwem informacji, a także nową dokumentacją w tym zakresie. Materiały te mają stanowić uniwersalne i praktyczne kompendium wiedzy, omawiające najistotniejsze zagadnienia związane z bezpieczeństwem informacji u Zamawiającego.
2. Szczegółowe programy szkolenia i ich dokładne terminy, a także materiały szkoleniowe zostaną zaproponowane przez Wykonawcę i będą wymagały akceptacji Zamawiającego.
3. Szkolenie zostanie przeprowadzone w siedzibie Zamawiającego (szkolenie stacjonarne).

VI. ETAP V

1. W ramach Etapu VI Wykonawca będzie świadczył usługę asysty w następującym zakresie:
   1) przeprowadzenie procesów:
      a) identyfikacji aktywów informacyjnych i klasyfikacji informacji przetwarzanych u Zamawiającego,
      b) szacowania ryzyka oraz postępowania z ryzykiem, związanych z utratą poufności, integralności i dostępności informacji przetwarzanych u Zamawiającego,
      - z udziałem wyznaczonych w tym celu pracowników Zamawiającego;
   2) wyjaśnianie zagadnień ujętych w SZBI i proponowanie rozwiązań w zakresie jego wdrażania;
   3) pomoc w rozwiązywaniu bieżących problemów, które mogą pojawić się w toku funkcjonowania SZBI;
   4) pomoc w modyfikacji dokumentacji Zamawiającego związanej z bezpieczeństwem informacji, w szczególności SZBI (np. poprzez zmianę poszczególnych elementów składowych lub opracowanie nowych elementów).

2. Usługi asysty świadczone będą zdalnie (w szczególności za pośrednictwem poczty elektronicznej lub telefonu) lub w siedzibie Zamawiającego. Decyzja o formie świadczenia Usług asysty zależeć będzie od ich charakteru i każdorazowo należy do Zamawiającego.

VII. Ogólna charakterystyka Zamawiającego:

1. Zamawiający, będący jednostką sektora finansów publicznych, realizuje m.in. zadania dotyczące ocen oddziaływania na środowisko, ochrony przyrody, zapobiegania szkodom w środowisku, odpowiada za zarządzanie informacją o środowisku przyrodniczym. Kompetencje Zamawiającego zostały określone w szczególności w następujących przepisach prawa powszechnie obowiązującego:
   1) ustawie z dnia 3 października 2008 r. o *udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowiska;*
   2) ustawie z dnia 16 kwietnia 2004 r. o *ochronie przyrody*;
   3) ustawie z dnia 27 kwietnia 2001 r. *Prawo ochrony środowiska;*
   4) ustawie z dnia 11 sierpnia 2021 r. *o gatunkach obcych;*
   5) ustawie z dnia 13 kwietnia 2007 r. o *zapobieganiu szkodom w środowisku i ich naprawie;*
2. Siedziba Zamawiającego znajduje się w Olsztynie. Ponadto posiada 3 placówki zamiejscowe w Elblągu, Ełku i Jeleniu, których pomieszczenia są wynajmowane.
3. Rejestry pozostające we właściwości Zamawiającego:
   - Rejestr form ochrony przyrody.
4. Struktura Organizacyjna Zamawiającego:
   1) Wydział Ocen Oddziaływania na Środowisko,
   2) Wydział Ochrony Przyrody i Obszarów Natura 2000,
   3) Wydział Zapobiegania i Naprawy Szkód w Środowisku oraz Informacji o Środowisku i Zarządzania Środowiskiem,
   4) Wydział Spraw Terenowych I w Elblągu,
   5) Wydział Spraw Terenowych II w Ełku,
   6) Wydział Organizacyjno – Administracyjny,
   7) Zespół Budżetu i Finansów,
   8) Pełnomocnik do spraw ochrony informacji niejawnych,
   9) Inspektor ochrony danych,
   10) Samodzielne stanowisko do spraw bezpieczeństwa i higieny pracy,
   11) Samodzielne stanowisko do spraw obronnych i zarządzania kryzysowego.
5. Przybliżona liczba pracowników Zamawiającego - 70 osób.
6. Pozostałe informacje dotyczące Zamawiającego dostępne są pod adresem: https://www.gov.pl/web/rdos-olsztyn