Opis Przedmiotu Zamówienia

(zwany „**OPZ**”)

I. Ogólne warunki realizacji zamówienia

1. Przedmiotem zamówienia jest opracowanie przez Wykonawcę dla Zamawiającego nowego systemu zarządzania bezpieczeństwem informacji, zwanego „**nowym SZBI**”, i przeprowadzenie szkoleń, zwanych „**Szkoleniami**”, oraz przekazanie materiałów szkoleniowych m.in. w zakresie jego funkcjonowania, a także świadczenie usług asysty wdrożeniowej, zwanych „**Usługami asysty**”, zgodnie z Umową, zwane „**Przedmiotem Umowy**”.

2. Przedmiot Umowy będzie realizowany w czterech etapach:

1) **Etap I** – analiza działalności Zamawiającego i sporządzenie Sprawozdania, o którym mowa w tyt. II ust. 1 pkt 2;
2) **Etap II** – opracowanie nowego SZBI;
3) **Etap III** – przeprowadzenie Szkoleń i przekazanie materiałów szkoleniowych, o których mowa w tyt. IV ust. 1 pkt 2;
4) **Etap IV** – 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

1. W ramach Etapu I 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) SZBI aktualnie funkcjonujący u Zamawiającego,

g) wstępną identyfikację informacji przetwarzanych u Zamawiającego,

h) 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 nowego SZBI – również poprzez weryfikację działalności

Zamawiającego m.in. w jego siedzibach (konieczność wizji lokalnej w dwóch lokalizacjach w Warszawie – adresy wskazano w tyt. VI ust. 2);

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 u niego nowego SZBI,

c) obejmujące wstępną koncepcję nowego 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 nowym SZBI.

2. W celu przeprowadzenia Analizy Zamawiający udostępni Wykonawcy niezbędne, posiadane dokumenty, w szczególności dotyczące aktualnie funkcjonującego SZBI.

3. Sprawozdanie zostanie przekazane Zamawiającemu w formie edytowalnego pliku elektronicznego (doc lub .docx) oraz w formie pisemnej.

4. Celem opracowania przez Wykonawcę wstępnej koncepcji nowego SZBI, Zamawiający wskazuje poniżej ogólny ramowy zarys nowego SZBI:

Określenie struktury dokumentacji nowego SZBI, która powinna mieć układ hierarchiczny, tj. opisywać nowy 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 nowego SZBI – z tym dokumentem powinny być spójne pozostałe dokumenty składające się na dokumentację nowego SZBI,

2) poziom systemów teleinformatycznych – polityka bezpieczeństwa systemów teleinformatycznych, na którą 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 GDOŚ,
- użytkowanie urządzeń mobilnych.

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

III. ETAP II

1. W ramach Etapu II Wykonawca, na podstawie wyników Analizy i zaakceptowanego przez Zamawiającego Sprawozdania, opracuje nowy SZBI, dostosowany do potrzeb Zamawiającego.

2. Nowy SZBI, który opracuje Wykonawca, będzie stanowił system zarządzania bezpieczeństwem informacji, o którym mowa w § 20 ust. 1 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2021 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. z 2017 r. poz. 2247), bądź w zastępujących go, odpowiednich przepisach wykonawczych do ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz. U. z 2021 r. poz. 2070, z późn. zm.), w przypadku ich nowelizacji, zwany „**SZBI**”. Rozporządzenie, o którym mowa w zdaniu poprzedzającym, zwane jest dalej „**rozporządzeniem KRI**”.

3. Nowy SZBI powinien być zgodny z rozporządzeniem KRI i spełniać wymagania 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, nowy SZBI powinien uwzględniać wymagania norm: PN-ISO/IEC 27002, PN-ISO/IEC 27005 oraz PN-ISO/IEC 24762.

4. Nowy SZBI musi być zgodny z aktualnymi przepisami powszechnie obowiązującego prawa, w tym w szczególności z przepisami:

1) rozporządzenia KRI;

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);

3) ustawy z dnia 10 maja 2018 r. *o ochronie danych osobowych* (Dz. U. z 2019 r. poz. 1781);

4) ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne*;

5) ustawy z dnia 6 września 2001 r. *o dostępie do informacji publicznej* (Dz. U. z 2020 r. poz. 2176, z późn. zm.);

6) 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* (Dz. U. z 2021 r. poz. 2373, z późn. zm.);

7) ustawy z dnia 5 sierpnia 2010 r. *o ochronie informacji niejawnych* (Dz. U. z 2019 r. poz. 742);

8) ustawy z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* (Dz. U. z 2020 r. poz. 1369, z późn. zm.);

oraz uwzględniać wewnętrzne akty prawne obowiązujące u Zamawiającego.

5. W ramach opracowania nowego SZBI Wykonawca między innymi:

1) zaproponuje obszary funkcjonalne, które powinny zostać objęte nowym SZBI, spójne z treścią Sprawozdania zaakceptowanego przez Zamawiającego;

2) uwzględni w szczególności następujące zagadnienia:

a) określenie organizacji bezpieczeństwa informacji,

b) identyfikacja aktywów informacyjnych i klasyfikacji informacji przetwarzanych u Zamawiającego,

c) szacowanie ryzyka oraz postępowanie 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,

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 bezpieczństwa 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 nowym SZBI przedstawi zestawienie, zwane „**Zestawieniem**, w którym wykaże spełnienie przez nowy SZBI wymagań dotyczących bezpieczeństwa informacji wynikających z aktualnych przepisów powszechnie obowiązującego prawa, w tym rozporządzenia KRI, a także odpowienich norm.

7. Nowy SZBI oraz Zestawienie zostaną przekazane Zamawiającemu w formie edytowalnego pliku elektronicznego (doc lub .docx) oraz w formie pisemnej.

8. Zamawiający zastrzega sobie prawo do każdorazowego wnoszenia uwag do zaproponowanego przez Wykonawcę nowego 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.

IV. ETAP III

1. W ramach Etapu III Wykonawca:

1) przeprowadzi dwa szkolenia (trwające min. 4h każde):

- dla kadry kierowniczej Zamawiającego (maksymalnie 20 osób) oraz
- dla osób odpowiedzialnych u Zamawiającego za funkcjonowanie SZBI (maksymalnie 15 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 szczególności poprzez przedstawienie Zamawiającemu głównych obszarów, poszczególnych ścieżek procedur i zasad reagownia na incydenty, wynikających z nowego 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 nowego 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 szkoleń i ich dokładne terminy, a także materiały szkoleniowe zostaną zaproponowane przez Wykonawcę i będą wymagały akceptacji Zamawiającego.

3. Szkolenia zostaną przeprowadzone w siedzibie Zamawiającego (szkolenia stacjonarne). W przypadku stanu epidemii wywołanego zakażeniami wirusem SARS-CoV-2 na terytorium Rzeczypospolitej Polskiej, uniemożliwiającego przeprowadzenie szkoleń stacjonarnych, Zamawiający może postanowić o przeprowadzeniu szkoleń za pośrednictwem środków komunikacji elektronicznej umożliwiających prozumiewanie się na odległość, wskazanych przez Zamawiającego (np. aplikacji *MS Teams*).

V. ETAP IV

1. W ramach Etapu IV Wykonawca będzie świadczył Usługi 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 nowym SZBI i proponowanie rozwiązań w zakresie jego wdrażania;

3) pomoc w rozwiązywaniu bieżących problemów, które mogą pojawić się w toku funkcjowania nowego SZBI;

4) pomoc w modyfikacji dokumentacji Zamawiającego związanej z bezpieczeństwem informacji, w szczególności nowego 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.

VI. Ogólna charakterystyka Zamawiającego:

1. Zamawiający, będący jednostką sektora finansów publicznych, jest instytucją ekspercką odpowiedzialną za ochronę przyrody i kontrolę procesu inwestycyjnego. Zamawiający w granicach swoich kompetencji realizuje m.in. zadania dotyczące zapobiegania szkodom w środowisku, odpowiada za zarządzanie informacją o środowisku przyrodniczym, rejestrację organizacji w systemie ekozarządzania i audytu (EMAS) oraz koordynuje prace sieci „Partnerstwo: Środowisko dla rozwoju w Polsce". 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 ochonie przyrody* (Dz. U. z 2021 r. poz. 1098, z późn. zm.);

3) ustawie z dnia 27 kwietnia 2001 r. *Prawo ochrony środowiska* (Dz. U. z 2021 r. poz. 1973, z późn. zm.);

4) ustawie z dnia 11 sierpnia 2021 r. *o gatunkach obcych* (Dz. U. poz. 1781);

5) ustawie z dnia 13 kwietnia 2007 r. *o zapobieganiu szkodom w środowisku i ich naprawie* (Dz. U. z 2021 r. poz. 2187).

2. Siedziba Zamawiającego – Zamawiający dysponuje powierzchnią biurową w budynkach niebędących jego własnością, zlokalizowanych pod następującymi adresami:
   1) ul. Wawelska 52/54, 00-922 Warszawa (część jednego piętra budynku);
   2) ul. Aleje Jerozolimskie 132/136, 02-305 Warszawa (dwa piętra w budynku Eurocentrum Alfa);

   - każdorazowo jednak, gdy w Umowie jest mowa o „siedzibie" (l. poj.) Zamawiającego, chodzi o siedzibę, o której mowa w pkt 2 powyżej.
3. Rejestry pozostające we właściwości Zamawiającego:
   1) Baza danych o ocenach oddziaływania na środowisko;
   2) Centralny Rejestr Form Ochrony Przyrody (CRFOP);
   3) Baza danych obszarów Natura 2000;
   4) Rejestr bezpośrednich zagrożeń szkodą w środowisku i szkód w środowisku;
   5) Rejestr historycznych zanieczyszczeń powierzchni ziemi;
   6) Rejestr organizacji zarejestrowanych w systemie ekozarządzania i audytu (EMAS);
   7) Internetowa przeglądarka mapowa informacji o środowisku i jego ochronie;
   8) Internetowy katalog metadanych o środowiskowych danych przestrzennych;
   9) Centralny Rejestr Danych o IGO;
   10) System Zarządzania Ochroną Przyrody;
   11) Bank Danych o Zasobach Przyrodniczych.
4. Struktura Organizacyjna Zamawiającego:
   1) Biuro Dyrektora Generalnego;
   2) Biuro Prawne;
   3) Departament Realizacji Projektów Środowiskowych;
   4) Departament Ocen Oddziaływania na Środowisko;
   5) Departament Orzecznictwa Administracyjnego;
   6) Departament Zarządzania Zasobami Przyrody;
   7) Zespół do spraw Budżetu i Finansów;
   8) Stanowisko ds. Audytu Wewnętrznego;
   9) Stanowisko ds. Ochrony Informacji Niejawnych.
5. Przybliżona liczba pracowników Zamawiającego to poniżej 200 osób.
6. Pozostałe informacje dotyczące Zamawiającego dostępne są pod adresem www.gov.pl/gdos.