Załącznik nr 1

OPIS PRZEDMIOTU ZAMÓWIENIA

Spis treści

I. WPROWADZENIE

Przedmiotem zamówienia jest opracowanie i wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (dalej: „**SZBI**") wraz z przeprowadzeniem szkoleń dla kadry zarządzającej oraz personelu IT w zakresie wdrożonego SZBI (dalej: „**Szkolenia**") oraz przeprowadzenie audytu zgodności z rozporządzeniem w sprawie Krajowych Ram Interoperacyjności (dalej: „**KRI**"), ustawą o Krajowym Systemie Cyberbezpieczeństwa (dalej: „**UoKSC**") w 10 jednostkach podległych Zamawiającemu (dalej: „**JP**").

Zamówienie jest finansowane w ramach Krajowego Planu Odbudowy i Zwiększania Odporności finansowanego ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności (dalej: „KPO"), Inwestycja C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo Cyberbezpieczeństwo - Cyberbezpieczny Rząd.

II. OPIS PRZEDMIOTU ZAMÓWIENIA

1. Zakres Przedmiotu zamówienia

1.1. Przedmiot zamówienia obejmuje wykonanie n/w zadań w JP Zamawiającego:
   1) Zadanie I – opracowanie i wdrożenie dokumentacji SZBI wraz z przeprowadzeniem Szkoleń;
   2) Zadanie II – przeprowadzenie audytu zgodności z KRI, UoKSC.

1.2. Wszystkie audyty, wdrożenia i szkolenia muszą uwzględniać aktualny stan prawny na dzień ich realizacji, w tym wymogi znowelizowanej UoKSC oraz aktualne przepisy KRI.

1.3. Realizacja Przedmiotu zamówienia odbywać się będzie w podziale na 10 części (zgodnie z wykazem w tabeli poniżej):

Część	Jednostka podległa	Lokalizacja	Adres strony internetowej	Szacunkowa liczba pracowników
1	Regionalna Dyrekcja Ochrony Środowiska w Łodzi	Ul. Traugutta 25, 90-113 Łódź	gov.pl/web/rdos-lodz	69
2	Regionalna Dyrekcja Ochrony Środowiska w Gdańsku	Ul. Chmielna 54/57, 80-748 Gdańsk	gov.pl/web/rdos-gdansk	104
		Oddział zamiejscowy w Słupsku Ul. Jana Pawła II 1, 76-200 Słupsk		
		Oddział zamiejscowy w Dziemianach Ul. 8 Marca 3, 83-425 Dziemiany		

3	Regionalna Dyrekcja Ochrony Środowiska w Gorzowie Wielkopolskim	Ul. Kosynierów Gdyńskich 78, 66-400 Gorzów Wielkopolski	gov.pl/web/rdos-gorzow	50
4	Regionalna Dyrekcja Ochrony Środowiska w Krakowie	Ul. Mogilska 25, 31-542 Kraków Wydział Spraw Terenowych w Tarnowie Al. Solidarności 5-9, 33-100 Tarnów Wydział Spraw Terenowych w Starym Sączu Ul. Daszyńskiego 3, 33-340 Stary Sącz	gov.pl/web/rdos-krakow	102
5	Regionalna Dyrekcja Ochrony Środowiska w Rzeszowie	al. Józefa Piłsudskiego 38, 35-001 Rzeszów Wydział Spraw Terenowych I w Krośnie (WST.KR) ul. Bieszczadzka 1, 38-400 Krosno Wydział Spraw Terenowych II w Przemyślu (WST.PRZ) ul. Kościuszki 2, 37-700 Przemyśl	gov.pl/web/rdos-rzeszow	95
6	Regionalna Dyrekcja Ochrony Środowiska w Lublinie	Ul. Bazylianówka 46, 20-144 Lublin Wydział Spraw Terenowych I Ul. Warszawska 14, 21-500 Biała Podlaska	gov.pl/web/rdos-lublin	82

		Wydział Spraw Terenowych II Pl. Niepodległości 1, 22-100 Chełm		
		Wydział Spraw Terenowych III ul. Partyzantów 3, 22-400 Zamość		
		Wydział Spraw Terenowych IV ul. Bohaterów Porytowego Wzgórza 35, 23-300 Janów Lubelski		
7	Regionalna Dyrekcja Ochrony Środowiska w Kielcach	Ul. Karola Szymanowskiego 6, 25-361 Kielce	gov.pl/web/rdos-kielce	56
8	Regionalna Dyrekcja Ochrony Środowiska w Poznaniu	Ul. Kościuszki 57, 61-891 Poznań	gov.pl/web/rdos-poznan	114
9	Regionalna Dyrekcja Ochrony Środowiska w Opolu	Ul. Firmowa 1, 45-594 Opole	gov.pl/web/rdos-opole	43
10	Regionalna Dyrekcja Ochrony Środowiska w Wrocławiu	Ul. Jana Długosza 68, 51-162 Wrocław	gov.pl/web/rdos-wroclaw	88

1.4. Wykonawca może złożyć ofertę na jedną lub kilka części.

2. Ogólna charakterystyka JP

2.1. Jednostki podległe – Regionalne Dyrekcje Ochrony Środowiska to wyspecjalizowane organy administracji rządowej, których działalność koncentruje się na ocenach oddziaływania na środowisko, ochronie przyrody oraz zapobieganiu szkodom w środowisku. Jednostki te odpowiadają również za kompleksowe zarządzanie informacją o środowisku przyrodniczym w podległych im regionach.

2.2. Kompetencje i zadania realizowane przez JP zostały określone w szczególności w następujących przepisach prawa powszechnie obowiązującego:

- Ustawa z dnia 3 października 2008 r. o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowisko;

- Ustawa z dnia 16 kwietnia 2004 r. o ochronie przyrody;
- Ustawa z dnia 27 kwietnia 2001 r. Prawo ochrony środowiska;
- Ustawa z dnia 11 sierpnia 2021 r. o gatunkach obcych;
- Ustawa z dnia 13 kwietnia 2007 r. o zapobieganiu szkodom w środowisku i ich naprawie.

2.3. Szczegółowa struktura zatrudnienia oraz wykaz komórek organizacyjnych każdej z JP są publicznie dostępne w Biuletynie Informacji Publicznej (BIP) na dedykowanych stronach JP, podanych w tabeli powyżej. W celu rzetelnego oszacowania prac, w szczególności struktury organizacyjnej oraz specyfiki realizowanych zadań publicznych, Wykonawca powinien zapoznać się z informacjami udostępnionymi w BIP poszczególnych JP.

III. SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. Wymagania minimalne dla zadań

1.1. Zadanie I: Opracowanie i wdrożenie dokumentacji SZBI wraz z przeprowadzeniem Szkoleń dla kadry zarządzającej oraz personelu IT w zakresie wdrożonego SZBI

1.1.1. Analiza stanu istniejącego:

1) Zamawiający wymaga przeprowadzenia analizy aktualnego stanu bezpieczeństwa informacji w JP, w tym procesów, procedur operacyjnych i mechanizmów kontroli związanych z bezpieczeństwem informacji, identyfikację zasobów informacyjnych, procesów przetwarzania danych oraz analizę luk.

1.1.2. Opracowanie pełnego zestawu dokumentów SZBI:

1) Zamawiający wymaga opracowania kompletnego zestawu dokumentów SZBI, w tym:
   a) Politykę Bezpieczeństwa Informacji,
   b) Politykę przetwarzania danych osobowych,
   c) Procedurę Bezpieczeństwa Fizycznego,
   d) Procedurę Bezpieczeństwa Teleinformatycznego,
   e) Procedurę zarządzania zdarzeniami i incydentami bezpieczeństwa,
   f) Procedurę identyfikacji informacji,
   g) Analizę i ocenę ryzyka oraz plan postępowania z ryzykiem,
   h) Procedurę szkoleń i podnoszenia świadomości użytkowników;
2) SZBI musi być dostosowane do realiów JP oraz jego charakterystyki;
3) SZBI powinno zostać napisane w sposób zwięzły, przystępnym językiem, umożliwiających łatwe zrozumienie i stosowanie zapisów w praktyce;
4) SZBI musi uwzględniać wymagania następujących norm oraz aktów prawnych (dalej: „**przepisy Cyber**”):
   a) PN-EN ISO/IEC 27001,
   b) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, ze zm.),

c) Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000, ze zm.),
d) Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2026 poz. 20 ze zm.),
e) 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 (NIS 2), zmieniająca rozporządzenie (UE) nr 910/2014 oraz uchylająca dyrektywę (UE) 2016/1148 (Dz. Urz. UE L 333 z 27.12.2022, str. 80),
f) Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej praz minimalnych wymagań dla systemów teleinformatycznych.
g) ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U z 2024 r. poz. 307 ze zm.) oraz aktami wykonawczymi do w/w ustawy.
h) inne właściwe przepisy prawa powszechnie obowiązującego, w szczególności z zakresu bezpieczeństwa informacji, ochrony danych osobowych oraz cyberbezpieczeństwa.

1.1.3. Wdrożenie SZBI:

1) przeprowadzenie warsztatów wprowadzających do wdrożenia SZBI z kierownictwem JP;
2) wdrożenie procedur operacyjnych i systemowych w zakresie SZBI;
3) wdrożenie rejestrów, formularzy i ewidencji wymaganych przepisami prawa.

1.1.4. Szkolenia:

1) przeprowadzenie specjalistycznego Szkolenia dla kluczowych pracowników (kadry zarządzającej oraz personelu IT) w JP, mające na celu praktyczne przygotowanie personelu do obsługi i nadzoru nad wdrożonym SZBI;
2) Szkolenie musi bazować na zindywidualizowanej dokumentacji (politykach, procedurach, instrukcjach) opracowanej dla danej JP, tak aby uczestnicy nabyli umiejętność korzystania z niej w codziennej pracy;
3) program Szkolenia musi uwzględniać specyficzne środki bezpieczeństwa technicznego i organizacyjnego zastosowane w danej JP;
4) wymagania organizacyjne dla Szkolenia:
   a) minimum 6 godzin dydaktycznych (po 45 minut),
   b) stacjonarnie w lokalizacjach JP lub zdalnie (po uzgodnieniu terminu z JP). Wybór trybu zdalnego nie może wpływać na jakość i rzetelność Szkolenia – musi ono zapewniać pełną interakcję z uczestnikami,
   c) treści przekazywane podczas Szkolenia muszą być sformułowane w sposób zwięzły i przystępny, tak aby skomplikowane wymogi normatywne były zrozumiałe dla osób niebędących specjalistami IT;
5) <u>minimalny zakres programowy szkolenia (bloki tematyczne):</u>
   a) wstęp do bezpieczeństwa informacji,

b) omówienie przepisów Cyber oraz obowiązków wynikających z wdrożonego SZBI,

c) omówienie struktury dokumentacji, ról i odpowiedzialności przypisanych pracownikom w JP,

d) omówienie wdrożonych instrukcji,

e) praktyczna instrukcja postępowania z ryzykiem w oparciu o wyniki przeprowadzonej analizy ryzyka dla JP,

f) przeszkolenie z zakresu ścieżki raportowania i klasyfikacji zdarzeń oraz incydentów zgodnie z nowymi procedurami,

g) prezentacja zasad odtwarzania systemów i weryfikacji kopii zapasowych wdrożonych w JP,

h) najpopularniejsze zagrożenia oraz analiza ataków cybernetycznych oraz przewodnik po metodach obrony organizacji.

6) materiały szkoleniowe i certyfikaty:

a) Wykonawca, najpóźniej w dniu Szkolenia, przekaże komplet materiałów szkoleniowych w formie elektronicznej (edytowalnej lub PDF) uczestnikom Szkolenia;

b) Wykonawca, po zakończonym Szkoleniu, przekaże listę uczestników Szkolenia oraz wyda każdemu uczestnikowi imienny certyfikat, zawierający: nazwę Szkolenia *„Szkolenie specjalistyczne dla kadry zarządzającej oraz personelu IT w zakresie wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)”*, dane uczestnika, datę wystawienia oraz formę szkolenia (stacjonarne/online), informację o czasie trwania, bloki tematyczne, podpis trenera prowadzącego; logotyp KPO oraz źródło finansowania (przekazane przez Zamawiającego).

1.2. Zadanie II: Przeprowadzenie audytu zgodności z wymaganiami KRI, UoKSC

1.2.1. Audyt ma na celu niezależną ocenę poziomu zgodności wdrożonego w JP systemu zarządzania bezpieczeństwem informacji z wymaganiami KRI, UoKSC, w szczególności w zakresie obowiązków organu publicznego;

1.2.2. Wykonawca przeprowadzi audyt zgodności z KRI, UoKSC, aktualnymi na dzień realizacji Przedmiotu zamówienia;

1.2.3. Zadanie obejmuje następujące etapy:

1) etap przygotowawczy:

a) analiza dostępnej dokumentacji dotyczącej bezpieczeństwa informacji, systemów teleinformatycznych oraz cyberbezpieczeństwa w danej JP,

b) przygotowanie planu audytu w oparciu o wytyczne normy ISO 19011:2018, KRI, UoKSC;

2) audyt zgodności z KRI:

a) ocena zgodności z § 15–20 KRI (w zakresie bezpieczeństwa informacji),

b) ocena spełnienia minimalnych wymagań dla systemów teleinformatycznych, rejestrów publicznych i wymiany informacji elektronicznej,

c) weryfikacja przypisania ról, sposobów autoryzacji, zarządzania dostępem, prowadzenia dzienników zdarzeń itp.

3) audyt zgodności z UoKSC:

a) przeprowadzenie audytu zgodności z wymaganiami UoKSC oraz aktów wykonawczych,
b) realizacja audytu zgodnie z wytycznymi z Szablonu sprawozdania z audytu zgodnego z *ustawą o krajowym systemie cyberbezpieczeństwa*.

4) opracowanie raportu dla danej JP (*każda JP odrębnie*), zawierającego:

a) opis przedmiotu i zakresu audytu danej JP,
b) identyfikację obowiązujących wymagań prawnych,
c) listę kluczowych niezgodności wraz z ich opisem;
d) ocenę stopnia spełnienia wymogów KRI, UoKSC,
e) analizę istotnych ryzyk,
f) rekomendacje oraz plan działań naprawczych i doskonalących,
g) wnioski końcowe dotyczące poziomu bezpieczeństwa informacji.

2. Wymagania ogólne dla zadań

2.1. Wykonawca jest zobowiązany do uwzględnienia w ramach realizacji zadań wymogów przepisów Cyber.

2.2. Wykonawca może realizować zadania I i II równolegle oraz niezależnie od siebie, pod warunkiem że nie wpłynie to negatywnie na jakość prac ani nie spowoduje opóźnienia w wykonaniu całości Przedmiotu Umowy.

2.3. Prace będą realizowane w siedzibach poszczególnych JP. Zamawiający dopuszcza wykonywanie zadań zdalnie (np. analiza dokumentacji, konsultacje) wyłącznie po uprzednim uzgodnieniu terminów w poszczególnych JP. Wybór trybu zdalnego nie może wpływać na rzetelność, jakość oraz kompletność realizowanych prac i produktów końcowych.

2.4. W przypadku konieczności zdalnego dostępu do zasobów sieciowych JP, Wykonawca zobowiązany jest do korzystania z bezpiecznych, szyfrowanych połączeń (VPN) uzgodnionych z działem IT danej JP.

2.5. Zamawiający nie dopuszcza, aby osoby realizujące Przedmiot zamówienia kopiowały, skanowały, fotografowały ani w inny sposób utrwalały dokumenty, które zostały mu udostępnione w celu realizacji zadań. W przypadku, gdy realizacja Przedmiotu zamówienia wymagała będzie pobrania dokumentów udostępnionych przez JP, osoby realizujące Przedmiot zamówienia zobowiązane będą do przechowywania ich wyłącznie na służbowych zasobach Wykonawcy. Dokumenty te muszą zostać niezwłocznie usunięte po wykonaniu zadań, nie później niż w chwili zakończenia realizacji Przedmiotu zamówienia.

2.6. Zamawiający wymaga, aby wymiana informacji drogą elektroniczną odbywała się w sposób gwarantujący poufność przekazywanych danych i dokumentów.

2.7. Wykonawca ponosi pełną odpowiedzialność za bezpieczeństwo danych przekazanych mu do wglądu w celu realizacji zadań.

2.8. W celu zapewnienia poufności danych, Wykonawca zobowiązany jest do stosowania następujących zasad komunikacji elektronicznej:

1) wszelka dokumentacja (raporty, analizy, polityki) musi być przesyłana w formie zaszyfrowanych archiwów (standard AES-256, format .zip lub .7z);
2) hasła do plików muszą być przekazywane oddzielnym kanałem komunikacji (wiadomość SMS na wskazany numer telefonu osoby upoważnionej);
3) zabrania się przesyłania hasła w tej samej wiadomości e-mail, w której znajduje się zaszyfrowany załącznik.

2.9. Zamawiający, po podpisaniu Umowy, przygotuje i przekaże wymagane przez Wykonawcę dane oraz dokumenty wyłącznie osobom wchodzących w skład zespołu Wykonawcy, który zostanie zgłoszony zgodnie z § 5 Umowy. Wykonawca i jego zespół, zobowiązani będą do zachowania poufności danych, niedopuszczania do ich utraty oraz nieudostępniania osobom trzecim. W każdym przypadku, gdy na etapie realizacji Przedmiotu Umowy wystąpi konieczność zmiany osób wchodzących w skład zespołu, o którym mowa w zdaniu pierwszym, Wykonawca dokona takiej zmiany zgodnie z § 5 Umowy.

2.10. Wszystkie wytworzone w trakcie realizacji Przedmiotu zamówienia dokumenty muszą zostać przekazane w formatach edytowalnych (np.: .docx, .xlsx) oraz w formacie .pdf, z uwzględnieniem zasad, o których mowa w pkt 2.7. oraz muszą zostać odpowiednio oznaczone zgodnie z Księgą Identyfikacji Wizualnej Krajowego Planu Odbudowy oraz Strategią promocji i informacji KPO. Wytyczne w zakresie oznaczenia dokumentów oraz wzory dokumentów są dostępne na stronie pod liniem: https://www.kpo.gov.pl/strony/o-kpo/dla-instytucji/dokumenty/strategia-promocji-i-informacji-kpo/. Oznaczenie powinno być widoczne na dokumentach elektronicznych w sposób czytelny, zapewniający identyfikację dokumentu jako elementu realizacji projektu KPO.

2.11. Całość dokumentacji oraz Szkolenia muszą być prowadzone w języku polskim, w sposób zwięzły i przystępny dla osób niebędących specjalistami IT.

3. Wymagania dotyczące kadry

3.1. Zamawiający wymaga, aby Przedmiot zamówienia został zrealizowany przez zespół zgłoszony przez Wykonawcę zgodnie z § 5 Umowy.

3.2. Zespół Wykonawcy musi składać się z co najmniej dwóch audytorów, z których co najmniej jeden spełnia łącznie następujące warunki:
1) posiada certyfikat określony w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. z 2018 r., poz. 1999);
2) posiada co najmniej 4 – letnie doświadczenie w zakresie przeprowadzania audytu w obszarach: SZBI lub KRI lub UoKSC lub normy ISO/IEC 27001 oraz w okresie ostatnich 5 lat przed wszczęciem postępowania wykonał co najmniej 3 audyty w obszarach: SZBI lub KRI lub UoKSC lub NIS2 lub ISO/IEC 27001.

3.3. Zamawiający wymaga zachowania ciągłości prac realizowanych przez zespół złożony z co najmniej trzech audytorów, z których każdy spełnia łącznie warunki wskazane w pkt 3.1.

3.4. Wykonawca zapewnia, że zespół realizujący Umowę będzie posiadał kwalifikacje adekwatne do przypisanych im czynności.

3.5. Wykonawca, a także osoby uczestniczące w realizacji Przedmiotu zamówienia, zobowiązane będą do złożenia oświadczenia o dochowaniu bezterminowo poufności w zakresie informacji pozyskanych w toku realizacji Przedmiotu zamówienia.

3.6. Zamawiający nie będzie ponosił kosztów dojazdów, zakwaterowania i wyżywienia osób wykonujących przedmiot Umowy.

4. Wymagania dotyczące ubezpieczenia

4.1. Zamawiający wymaga, aby Wykonawca przez cały okres realizacji przedmiotu zamówienia posiadał ważne ubezpieczenie OC w zakresie prowadzonej działalności na kwotę nie mniejszą niż 200.000,00 zł (słownie: dwieście tysięcy złotych), obejmującego szkody mogące wyniknąć w związku z realizacją Przedmiotu zamówienia, w tym szkody osobowe, majątkowe oraz związane z utratą lub uszkodzeniem dokumentów i danych.

4.2. Kopię polisy Wykonawca zobowiązany będzie przedłożyć Zamawiającemu przed zawarciem Umowy, w celu jej dołączenia do umowy.

4.3. Wykonawca zobowiązany będzie do kontynuowania ubezpieczenia, o którym mowa w pkt 4.1, przez cały okres obowiązywania Umowy.

4.4. W przypadku, gdy okres ubezpieczenia upływa wcześniej niż termin zakończenia realizacji umowy, Wykonawca zobowiązany będzie przedłożyć Zamawiającemu, nie później niż ostatniego dnia obowiązywania ubezpieczenia, kopię dowodu jego przedłużenia.

4.5. W przypadku niedostarczenia potwierdzenia posiadania aktualnej polisy ubezpieczenia zgodnie z zapisami pkt 4.4, Zamawiający będzie uprawniony do naliczenia kary umownej, na zasadach określonych w umowie.