Załącznik nr 1

OPIS PRZEDMIOTU ZAMÓWIENIA

Spis treści

I. WPROWADZENIE

Przedmiotem zamówienia jest przeprowadzenie audytu Systemu Zarządzania Bezpieczeństwem Informacji (dalej: „**audyt SZBI**”) oraz przeprowadzenie audytu zgodności z rozporządzeniem w sprawie Krajowych Ram Interoperacyjności (dalej: „**KRI**”), ustawą o Krajowym Systemie Cyberbezpieczeństwa (dalej: „**UoKSC**”) w 6 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 – przeprowadzenie audytu SZBI;
   2) Zadanie II – przeprowadzenie audytu zgodności z KRI, UoKSC.

1.2. Wszystkie audyty 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 6 części (zgodnie z wykazem w tabeli poniżej):

Część	Jednostka podległa	Lokalizacja	Adres strony internetowej	Szacunkowa liczba pracowników
1	Regionalna Dyrekcja Ochrony Środowiska w Warszawie	ul. Henryka Sienkiewicza 3 00-015 Warszawa	gov.pl/web/rdos-warszawa	145
		Wydział Spraw Terenowych w Ciechanowie, Plac Tadeusza Kościuszki 5, 06-400 Ciechanów		
		Wydział Spraw Terenowych w Ciechanowie, Oddział w Płocku, ul. Kolegialna 15 (pokój 22 i 23), 09-402 Płock		
		Wydział Spraw Terenowych w Siedlcach,		

		ul. Kazimierzowska 9, 08-110 Siedlce Wydział Spraw Terenowych w Siedlcach, Oddział w Ostrołęce, ul. Berka Joselewicza 1, 07-410 Ostrołęka Wydział Spraw Terenowych w Radomiu, ul. 25 Czerwca 68, 26-600 Radom		
2	Regionalna Dyrekcja Ochrony Środowiska w Białymstoku	ul. Dojlidy Fabryczne 23 15-554 Białystok Wydział Spraw Terenowych I w Suwałkach ul. Utrata 9A, 16-400 Suwałki Wydział Spraw Terenowych II w Łomży ul. Nowa 2, 18-400 Łomża	gov.pl/web/rdos-bialystok	62
3	Regionalna Dyrekcja Ochrony Środowiska w Olsztynie	ul. Dworcowa 60 10-437 Olsztyn Wydział Spraw Terenowych I ul. Wojska Polskiego 1 Wydział Spraw Terenowych II ul. Kolonia 1, 19-300 Ełk	gov.pl/web/rdos-olsztyn	78
4	Regionalna Dyrekcja Ochrony Środowiska w Bydgoszczy	ul. Dworcowa 81 85-009 Bydgoszcz Wydział Spraw Terenowych delegatura we Włocławku ul. Brzeska 6 87-800 Włocławek	gov.pl/web/rdos-bydgoszcz	70
5	Regionalna Dyrekcja Ochrony Środowiska w Szczecinie	ul. Juliusza Słowackiego 2 71-434 Szczecin Wydział Spraw Terenowych w Koszalinie	gov.pl/web/rdos-szczecin	81

		ul. 1 Maja 36, 75-001 Koszalin Wydział Spraw Terenowych w Złocieńcu ul. Dworcowa 13, 78-520 Złocieniec		
6	Regionalna Dyrekcja Ochrony Środowiska w Katowicach	Plac Grunwaldzki 8/10 40-127 Katowice	gov.pl/web/rdos-katowice	74

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 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, 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 – audyt SZBI

1.1.1. Audyt ma na celu niezależną ocenę poziomu zgodności i dojrzałości SZBI oraz skuteczności wdrożonych zabezpieczeń organizacyjnych i technicznych.

1.1.2. Zadanie obejmuje w szczególności:

1) etap przygotowawczy:

a) analiza dostępnej dokumentacji SZBI, w tym polityk, procedur, rejestrów, planów oraz wcześniejszych przeglądów i ocen ryzyka,

b) przygotowanie planu audytu w oparciu o wytyczne normy PN-ISO/IEC 27007:2020 oraz ISO 19011:2018;

2) przeprowadzenie audytu SZBI:

a) weryfikacja zgodności wdrożonego SZBI z wymaganiami normy PN-ISO/IEC 27001:2022 – analiza klauzul 4–10 oraz załącznika A (kontrole z PN-ISO/IEC 27002:2022),
b) ocena poziomu wdrożenia i skuteczności mechanizmów zarządzania ryzykiem, ciągłości działania, kontroli dostępu, zarządzania incydentami, zasobami IT itd.,
c) wywiady z właścicielami procesów, zespołem IT oraz osobami odpowiedzialnymi za bezpieczeństwo informacji;

3) opracowanie raportu końcowego z audytu (*dla każdej JP odrębnie*) zawierającego:

a) opis przebiegu audytu;
b) identyfikację niezgodności i obszarów do poprawy;
c) rekomendacje i priorytety działań naprawczych;
d) ocenę poziomu zgodności z PN-ISO/IEC 27001:2022, KRI i UoKSC.

1.2. Zadanie I – audyt 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 audytów

2.1. Wykonawca jest zobowiązany do uwzględnienia w ramach realizacji Przedmiotu zamówienia wymogów m.in. norm i przepisów:
1) PN-EN ISO/IEC 27001,
2) 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.),
3) Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000, ze zm.),
4) Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2026 poz. 20 ze zm.),
5) 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),
6) 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.
7) 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.
8) innych właściwych przepisów prawa powszechnie obowiązującego, w szczególności z zakresu bezpieczeństwa informacji, ochrony danych osobowych oraz cyberbezpieczeństwa.

2.2. 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.

2.3. 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.

2.4. 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.

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

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

2.7. 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;

2.8. 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 i Wizualizacji 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.

2.9. 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 kierowany przez co najmniej jednego audytora wiodącego, który 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) w okresie ostatnich 3 lat przed wszczęciem postępowania wykonał co najmniej 3 audyty w obszarach: KRI lub UoKSC lub ISO 27001 lub ISO 22301.

3.2. Wykonawca po podpisaniu umowy przekaże Zamawiającemu listę zespołu skierowanego do realizacji zamówienia.

3.3. Zamawiający wymaga zachowania ciągłości prac realizowanych przez zespół, o którym mowa w pkt 3.2., w szczególności audytora wiodącego, o którym mowa w pkt 3.1.

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

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.