Załącznik nr 1 do zapytania ofertowego

OPIS PRZEDMIOTU ZAMÓWIENIA

Znak sprawy: BDG-ZZP.082.____.2026

I. WPROWADZENIE

1. **Przedmiot zamówienia**

1.1. Przedmiotem zamówienia jest przygotowanie i przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa (SZBI, NIS2/KSC, ciągłość działania oraz bezpieczne wykorzystanie narzędzi sztucznej inteligencji) dla kadry zarządzającej oraz pracowników Generalnej Dyrekcji Ochrony Środowiska i Regionalnych Dyrekcji Ochrony Środowiska.

1.2. Zamówienie finansowane jest 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.

2. **Cel szkoleń**

2.1. Celem szkoleń jest przygotowanie kadry zarządzającej oraz pracowników merytorycznych Zamawiającego i Regionalnych Dyrekcji Ochrony Środowiska, w tym pracujących z danymi wrażliwymi, do:

2.1.1. wypełniania obowiązków wynikających z dyrektywy NIS2[1] oraz ustawy o krajowym systemie cyberbezpieczeństwa[2], w tym w zakresie odpowiedzialności kierownictwa za zarządzanie ryzykiem;

2.1.2. praktycznego utrzymania Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz zapewnienia ciągłości działania;

2.1.3. bezpiecznego korzystania z narzędzi sztucznej inteligencji w środowisku pracy, z uwzględnieniem ryzyka wycieku danych;

2.1.4. rozpoznawania zagrożeń typowych dla administracji publicznej i właściwego reagowania na incydenty.

2.2. Szkolenia stanowią pierwszy, ogólny i uświadamiający etap przygotowania kadr Zamawiającego i Regionalnych Dyrekcji Ochrony Środowiska do realizacji obowiązków wynikających z ustawy o krajowym systemie cyberbezpieczeństwa.

2.3. Szkolenia nie obejmują ćwiczeń. W blokach 2 i 3 Wykonawca wprowadza pojęcia stosowane w Systemie Zarządzania Bezpieczeństwem Informacji Zamawiającego tj. właściciel procesu, właściciel systemu, Administrator Merytoryczny Systemu (AMS), koordynator ciągłości działania, pełnomocnik ds. bezpieczeństwa informacji (PBI), administrator bezpieczeństwa teleinformatycznego (ABT), inspektor ochrony danych (IOD), analiza wpływu na działalność (BIA), RTO i RPO – na poziomie ogólnym, bez przeprowadzania analiz.

II. OPIS PRZEDMIOTU ZAMÓWIENIA

3. Zakres ilościowy i forma

3.1. Zakres ilościowy i formę szkoleń określa poniższa tabela:

Lp.	Forma	Liczba sesji	Liczebność grupy	Czas trwania sesji
1.	stacjonarnie – siedziba Zamawiającego, Al. Jerozolimskie 136, Warszawa	2	do 30 osób	6 godzin zegarowych (9:00–15:00)
2.	online – platforma zapewniona przez Wykonawcę	3	do 80 osób	6 godzin zegarowych (9:00–15:00)
Razem		**5**	**do 300 osób**	

3.2. Wszystkie sesje realizowane są według tej samej agendy, dostosowanej do profilu grupy wskazanego przez Zamawiającego (kadra zarządzająca, pracownicy merytoryczni, grupa ogólna).

4. Minimalny zakres merytoryczny

4.1. Każda sesja obejmuje co najmniej następujące bloki tematyczne (zakres jednakowy dla każdej sesji):

Blok	Tematyka	Minimalny czas
1	NIS2 / KSC: nowe ramy prawne, rola GDOŚ i RDOŚ w świetle nowelizacji przepisów, odpowiedzialność kadry zarządzającej, obowiązki raportowe i dokumentacyjne	60 min
2	SZBI w codziennej pracy: socjotechnika, ochrona haseł i uwierzytelnianie wieloskładnikowe (MFA), bezpieczna praca zdalna, zgłaszanie incydentów	60 min
3	Ciągłość działania: rola planów ciągłości działania i planów odtwarzania, postępowanie w sytuacji kryzysowej, odpowiedzialność pracowników i kierownictwa	60 min
4	Bezpieczne wykorzystanie AI: ryzyka dużych modeli językowych (LLM), w tym wyciek danych; „shadow AI” (korzystanie z narzędzi AI poza wiedzą i kontrolą urzędu); rozpoznawanie deepfake’ów; bezpieczne formułowanie poleceń (promptów); dobre praktyki AI w urzędzie	60 min
5	Warsztat / case study: analiza realnych zagrożeń dla administracji publicznej oraz co najmniej 1 ćwiczenie – symulacja incydentu (np. ransomware) z omówieniem decyzji i błędów	45 min
6	Test wiedzy (quiz 10–15 pytań, może być online) z omówieniem wyników oraz sesja pytań i odpowiedzi	30 min

4.2. **Każdy z bloków 1–4 trwa co najmniej 60 minut. Łączny czas przerw w każdej sesji wynosi 45 minut. Sesja trwa 6 godzin zegarowych (9:00–15:00), w tym 315 minut zajęć merytorycznych.**

4.3. Ramowy harmonogram sesji (Wykonawca może zaproponować inny podział, z zachowaniem minimalnego czasu bloków i łącznego czasu przerw):

Godziny	Blok / przerwa
09:00–10:00	Blok 1 – NIS2 / KSC
10:00–11:00	Blok 2 – SZBI w codziennej pracy
11:00–11:15	*Przerwa (15 min)*
11:15–12:15	Blok 3 – Ciągłość działania
12:15–12:45	*Przerwa (30 min)*
12:45–13:45	Blok 4 – Bezpieczne wykorzystanie AI
13:45–14:30	Blok 5 – Warsztat / symulacja incydentu
14:30–15:00	Blok 6 – Test wiedzy, pytania i odpowiedzi

III. SZCZEGÓŁOWE WYMAGANIA

5. **Organizacja szkoleń**

5.1. **Wymaganie konieczne:** szkolenia odbędą się w następujących terminach, w godzinach 9:00–15:00:

Lp.	Termin (godz. 9:00–15:00)	Forma szkolenia
1.	**7.12.2026 r. (poniedziałek)**	online – platforma Wykonawcy
2.	**8.12.2026 r. (wtorek)**	stacjonarnie – siedziba Zamawiającego
3.	**2.12.2026 r. (środa)**	online – platforma Wykonawcy
4.	**3.12.2026 r. (czwartek)**	stacjonarnie – siedziba Zamawiającego
5.	**4.12.2026 r. (piątek)**	online – platforma Wykonawcy

5.2. Oferta, w której Wykonawca nie zagwarantuje przeprowadzenia szkoleń w terminach wskazanych w pkt 5.1, zostanie odrzucona jako niezgodna z warunkami zamówienia. Zmiana terminów jest możliwa wyłącznie w drodze zmiany treści zapytania ofertowego (przed upływem terminu składania ofert) albo na zasadach zmiany umowy określonych w projektowanych postanowieniach umowy.

5.3. Przydział grup uczestników do poszczególnych sesji ustala Zamawiający. Realizacja całego przedmiotu zamówienia, wraz z wystawieniem certyfikatów i przekazaniem raportu poszkoleniowego, nastąpi do dnia 11 grudnia 2026 r.

5.4. Zamawiający zapewnia dla sesji stacjonarnych salę szkoleniową z wyposażeniem multimedialnym (projektor/ekran, dostęp do Internetu).

5.5. Wykonawca zapewnia dla sesji online platformę umożliwiającą: prezentację materiałów, interakcję z uczestnikami (czat, pytania, ankiety/quiz), przeprowadzenie ćwiczenia oraz wygenerowanie raportu obecności uczestników; dostęp do platformy nie może wymagać instalacji oprogramowania ani zakupu licencji przez uczestników. Wykonawca zapewnia wsparcie techniczne w trakcie każdej sesji online.

5.6. Imienną listę uczestników wraz z adresami e-mail Zamawiający przekaże Wykonawcy niezwłocznie po zawarciu umowy, nie później niż na 1 dzień roboczy przed pierwszym

szkoleniem, a jej aktualizację – nie później niż na 1 dzień roboczy przed danym szkoleniem.

6. **Osoba prowadząca szkolenia**

6.1. Szkolenia prowadzi trener wskazany przez Wykonawcę na potwierdzenie spełnienia warunku udziału w postępowaniu (trener prowadzący), posiadający łącznie: certyfikat Audytora Wiodącego Systemu Zarządzania Bezpieczeństwem Informacji wg normy ISO/IEC 27001 (edycja 2013 lub 2022), wydany przez akredytowaną jednostkę certyfikującą, lub 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) (lub certyfikat równoważny) oraz certyfikat Audytora Wiodącego Systemu Zarządzania Ciągłością Działania wg normy ISO 22301 (edycja 2012 lub 2019), wydany przez akredytowaną jednostkę certyfikującą (lub certyfikat równoważny) albo – zamiast tego certyfikatu – udokumentowane doświadczenie w przeprowadzeniu, w okresie ostatnich 3 lat przed upływem terminu składania ofert, co najmniej 2 szkoleń, audytów lub wdrożeń z zakresu zarządzania ciągłością działania, w których trener był osobą prowadzącą lub członkiem zespołu, zgodnie z rozdziałem IV zapytania ofertowego. Spełnienie tego wymagania Wykonawca potwierdza w wykazie osób (część II Formularza ofertowego), w którym podaje dane posiadanych certyfikatów lub doświadczenia.

6.2. Doświadczenie trenera prowadzącego w przeprowadzaniu szkoleń z zakresu cyberbezpieczeństwa / SZBI dla podmiotów publicznych podlega ocenie w kryterium oceny ofert określonym w zapytaniu ofertowym.

6.3. Zmiana trenera prowadzącego jest dopuszczalna wyłącznie na zasadach określonych w umowie.

7. **Obowiązki Wykonawcy**

7.1. Przekazanie Zamawiającemu do akceptacji, niezwłocznie po zawarciu umowy, najpóźniej do godz. 12:00 w dniu roboczym poprzedzającym pierwsze szkolenie: materiałów szkoleniowych dla uczestników w formacie PDF, w języku polskim, szczegółowego programu i harmonogramu szkolenia z podziałem na godziny i bloki tematyczne, treści testu wiedzy oraz wzoru imiennego certyfikatu.

7.2. Uwzględnienie uwag Zamawiającego, zgłoszonych w terminie 1 dnia roboczego od dnia otrzymania dokumentów (a w przypadku ich otrzymania w dniu roboczym poprzedzającym pierwsze szkolenie – w tym samym dniu), i przekazanie poprawionych dokumentów przed rozpoczęciem pierwszego szkolenia.

7.3. Przeprowadzenie w każdej sesji co najmniej jednego ćwiczenia (symulacji incydentu) oraz testu wiedzy.

7.4. Wystawienie po każdym szkoleniu, w terminie 3 dni roboczych, imiennych certyfikatów w formie elektronicznej i przesłanie ich na adresy e-mail uczestników oraz zbiorczo Zamawiającemu wraz z zestawieniem wystawionych certyfikatów. Certyfikat zawiera co najmniej: imię i nazwisko uczestnika, nazwę szkolenia i zakres tematyczny, datę, miejsce/tryb, liczbę godzin, dane Wykonawcy i prowadzącego oraz podstawę wydania.

7.5. Przekazanie Zamawiającemu, w terminie 3 dni roboczych od zakończenia ostatniego szkolenia: list obecności (sesje stacjonarne), raportów z platformy potwierdzających uczestnictwo (sesje online) oraz raportu poszkoleniowego zawierającego daty szkoleń, liczbę uczestników, agendę i zbiorcze wyniki testu wiedzy. Zbiorcze wyniki testu wiedzy obejmują, osobno dla każdego szkolenia: liczbę osób, które wypełniły test, średni wynik oraz odsetek poprawnych odpowiedzi na każde pytanie. Test jest anonimowy, a jego wynik nie wpływa na wydanie certyfikatu.

7.6. Oznakowanie materiałów (w tym slajdu tytułowego prezentacji i strony tytułowej materiałów PDF), certyfikatów i raportu zgodnie z zasadami promocji i oznakowania KPO oraz Księgą Identyfikacji Wizualnej KPO (https://www.gov.pl/web/cppc/cyberbezpieczny-rzad, zakładka „Materiały informacyjno-promocyjne").

7.7. Przeniesienie na Zamawiającego autorskich praw majątkowych do materiałów szkoleniowych (z licencją na wcześniejszy dorobek Wykonawcy) oraz przetwarzanie danych osobowych uczestników (imię i nazwisko, miejsce pracy, służbowy adres e-mail) wyłącznie w celu realizacji zamówienia – na zasadach określonych w projektowanych postanowieniach umowy.

7.8. Poddanie się kontroli instytucji uprawnionych do kontroli realizacji KPO oraz udostępnienie dokumentów związanych z realizacją zamówienia, na zasadach określonych w umowie.

8. Wymagania ogólne

8.1. **Produkty i usługi ICT.** Platforma do szkoleń online oraz inne produkty, usługi i procesy ICT wykorzystywane przez Wykonawcę do realizacji zamówienia, według stanu na dzień składania ofert i przez cały okres realizacji zamówienia, nie mogą obejmować typów produktów ICT, rodzajów usług ICT ani konkretnych procesów ICT dostarczanych przez dostawcę uznanego za dostawcę wysokiego ryzyka decyzją, o której mowa w art. 67b ust. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r. poz. 20, ze zm.), w zakresie objętym tą decyzją (art. 67c ust. 1 pkt 1 tej ustawy). Wykonawca wskazuje platformę w formularzu ofertowym.

8.2. **Zasada DNSH.** Przedmiot zamówienia jest zgodny z zasadą „nie czyń znaczącej szkody" (DNSH) – realizacja części szkoleń online oraz przekazywanie materiałów, certyfikatów i raportów wyłącznie w postaci elektronicznej ogranicza zużycie papieru i emisje związane z dojazdami.

8.3. **Język.** Szkolenia, materiały, test wiedzy, certyfikaty i raport sporządza się w języku polskim, w sposób przystępny dla osób spoza obszaru IT.

9. Odbiór

9.1. Odbiór przedmiotu zamówienia nastąpi na podstawie protokołu odbioru sporządzonego po zakończeniu ostatniego szkolenia, przekazaniu dokumentów, o których mowa w pkt 7.5, oraz certyfikatów wszystkim uczestnikom.

[1] 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 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80).

[2] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r. poz. 20, ze zm.).