

OPIS PRZEDMIOTU ZAMÓWIENIA

Spis treści

I. WPROWADZENIE

II. OPIS PRZEDMIOTU ZAMÓWIENIA

1. Zakres Przedmiotu zamówienia
2. Ogólna charakterystyka Zamawiającego i uczestników Szkoleń

III. SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. Wymagania minimalne dla zakresu merytorycznego Szkoleń
2. Wymagania ogólne dla realizacji Szkoleń
3. Wymagania dotyczące kadry
4. Produkty Przedmiotu zamówienia i odbiór
5. Prawa autorskie

I. WPROWADZENIE

Przedmiotem zamówienia jest przygotowanie i przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa (dalej: „Szkolenia” lub „Szkolenie”) dla kadry zarządzającej oraz pracowników merytorycznych pracujących z danymi wrażliwymi, zatrudnionych w Generalnej Dyrekcji Ochrony Środowiska (dalej: „Zamawiający” lub „GDOŚ”) oraz w jednostkach podległych Zamawiającemu – regionalnych dyrekcjach ochrony środowiska (dalej: „JP” lub „RDOŚ”).

Zakres Szkoleń obejmuje praktyczne utrzymanie Systemu Zarządzania Bezpieczeństwem Informacji (dalej: „SZBI”), wymagania wynikające z dyrektywy NIS2 oraz z ustawy o krajowym systemie cyberbezpieczeństwa (dalej: „UoKSC”), a także zarządzanie ciągłością działania oraz bezpieczne wykorzystanie narzędzi sztucznej inteligencji (dalej: „AI”) w środowisku pracy.

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 przeprowadzenie 5 sesji szkoleniowych o tożsamym zakresie merytorycznym. Grupy szkoleniowe mają charakter mieszany – w każdej sesji uczestniczą zarówno osoby z kadry zarządzającej (kierowniczej), jak i pracownicy merytoryczni. Wykonawca zapewni, aby każda sesja obejmowała zarówno obowiązki pracownika, jak i odpowiedzialność kierownictwa, w sposób czytelny dla obu tych grup. Podział sesji przedstawia poniższa tabela:

Lp.	Forma realizacji	Uczestnicy	Liczba sesji	Liczebność grupy	Czas trwania
1.	Stacjonarna – w siedzibie Zamawiającego w Warszawie	wyłącznie pracownicy GDOŚ – grupy mieszane (kadra zarządzająca i pracownicy merytoryczni)	2	do 30 osób	do 6 godzin zegarowych
2.	Online – na platformie Wykonawcy	wyłącznie pracownicy JP – RDOŚ – grupy mieszane (kadra kierownicza i pracownicy)	3	do 80 osób	do 6 godzin zegarowych

- 1.2. Wszystkie Szkolenia muszą uwzględniać aktualny stan prawny na dzień ich realizacji, w tym wymogi znowelizowanej UoKSC, dyrektywy NIS2 oraz aktualne przepisy KRI.
- 1.3. Każde Szkolenie obejmuje co najmniej jedno ćwiczenie / symulację incydentu oraz test wiedzy na zakończenie, wraz z omówieniem wyników.
- 1.4. Termin realizacji Przedmiotu zamówienia: do dnia 30 listopada 2026 r.
- 1.5. Zamawiający proponuje następujący harmonogram sesji szkoleniowych:

Nr	Proponowany termin	Forma	Grupa docelowa	Godziny
1.	05.11.2026 (czwartek)	stacjonarna	GDOŚ – grupa mieszana I	09:00–15:00
2.	10.11.2026 (wtorek)	stacjonarna	GDOŚ – grupa mieszana II	09:00–15:00
3.	17.11.2026 (wtorek)	online	RDOŚ – grupa mieszana I	09:00–15:00
4.	19.11.2026 (czwartek)	online	RDOŚ – grupa mieszana II	09:00–15:00
5.	24.11.2026 (wtorek)	online	RDOŚ – grupa mieszana III	09:00–15:00

- 1.6. Terminami rezerwowymi, wykorzystywanymi wyłącznie w razie konieczności przesunięcia którejkolwiek z sesji, są 26, 27 oraz 30 listopada 2026 r. Harmonogram ma charakter propozycji – ostateczne terminy zostaną uzgodnione przez Strony po zawarciu umowy, z zachowaniem terminu, o którym mowa w pkt 1.4. Zamawiający wskazuje, że 11 listopada 2026 r. (środa) jest dniem ustawowo wolnym od pracy.

2. Ogólna charakterystyka Zamawiającego i uczestników Szkoleń

- 2.1. Zamawiający oraz JP 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.
- 2.2. Uczestnikami Szkoleń są, z zachowaniem poniższego podziału na formy realizacji:

- 1) Szkolenia stacjonarne – wyłącznie pracownicy GDOŚ, w dwóch grupach mieszanych, obejmujących kadre zarządzającą GDOŚ oraz pracowników merytorycznych pracujących z danymi wrażliwymi;
 - 2) Szkolenia online – wyłącznie pracownicy JP (RDOŚ), w trzech grupach mieszanych, obejmujących kadre kierowniczą RDOŚ oraz pracowników RDOŚ;
 - 3) w każdej z grup mogą uczestniczyć PBI oraz pracownicy komórek właściwych do spraw informatyki – w zakresie koordynacji obsługi zgłoszeń i incydentów oraz uruchamiania procedur ciągłości działania;
 - 4) z uwagi na mieszany charakter grup Wykonawca zobowiązany jest prowadzić zajęcia w sposób umożliwiający równoległy odbiór treści przez obie kategorie uczestników – zagadnienia dotyczące odpowiedzialności kierownictwa (w szczególności z bloku II oraz decyzje w ramach ciągłości działania z bloku IV) omawiane są z jednoczesnym wskazaniem, jakie obowiązki wynikają z nich dla pracownika.
- 2.3. Szacunkowa łączna liczba uczestników Szkoleń wynosi do 300 osób, w tym do 60 pracowników GDOŚ (Szkolenia stacjonarne) oraz do 240 pracowników RDOŚ (Szkolenia online). Ostateczna liczba uczestników poszczególnych sesji, imienna lista uczestników oraz ich służbowe adresy e-mail zostaną przekazane Wykonawcy nie później niż na 5 dni roboczych przed terminem rozpoczęcia pierwszego Szkolenia.
- 2.4. Uczestnicy Szkoleń nie są specjalistami z obszaru IT; materiały i sposób prowadzenia zajęć muszą być dostosowane do odbiorcy nietechnicznego, z wykorzystaniem przykładów z administracji publicznej.

III. SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. Wymagania minimalne dla zakresu merytorycznego Szkoleń

1.1. Blok I – SZBI: praktyczne utrzymanie systemu w organizacji

- 1) rola pracownika i kierownictwa w SZBI, procesy bezpieczeństwa informacji;
- 2) podział odpowiedzialności pomiędzy Pełnomocnika ds. Bezpieczeństwa Informacji (dalej: „PBI”), Inspektora Ochrony Danych (dalej: „IOD”) oraz komórkę właściwą do spraw informatyki (dalej: „komórka IT”) – kto za co odpowiada i w jakiej kolejności podejmowane są działania;
- 3) ścieżka zgłaszania i eskalacji – od zgłoszenia pracownika, przez rejestrację w systemie zgłoszeń, po decyzje PBI i kierownictwa; kanały zgłoszeń obowiązujące u Zamawiającego;
- 4) czego komórka IT potrzebuje od pracownika przy zgłoszeniu incydentu (zakres informacji, zabezpieczenie śladów, czego nie należy robić samodzielnie);
- 5) cyberbezpieczeństwo w codziennej pracy, socjotechnika i phishing;
- 6) ochrona haseł, polityki dostępowe, uwierzytelnianie wieloskładnikowe (MFA);
- 7) bezpieczna praca zdalna i praca z danymi wrażliwymi;
- 8) zgłaszanie incydentów – ścieżka postępowania i obowiązki pracownika, w tym terminy wynikające z UoKSC.

- 1.1.1. W ramach bloku I Wykonawca precyzyjnie omówi role związane z systemami teleinformatycznymi i zasobami informacyjnymi Zamawiającego, wskazując granicę pomiędzy decyzją a jej wykonaniem oraz konsekwencje jej zatarcia:

Rola	Zakres odpowiedzialności	Czego rola NIE obejmuje
Właściciel biznesowy (właściciel zasobu / systemu)	Kierujący komórką organizacyjną, której zadania wspiera system. Odpowiada za cel istnienia systemu i zakres przetwarzanych w nim informacji, klasyfikację informacji, akceptację ryzyka, zatwierdzanie zakresu uprawnień (kto i w jakim zakresie ma dostęp), określenie wymagań ciągłości działania (RTO, RPO, priorytet odtwarzania), akceptację zmian i odbiór testów, decyzje o rozwoju i wycofaniu systemu.	Nie konfiguruje systemu, nie nadaje technicznie uprawnień, nie odpowiada za rozwiązania techniczne ani za utrzymanie infrastruktury.
Administrator merytoryczny (administrator funkcjonalny / danych)	Wyznaczony pracownik komórki merytorycznej. Realizuje decyzje właściciela biznesowego w warstwie funkcjonalnej: prowadzi konfigurację merytoryczną i słowniki, obsługuje wnioski o dostęp zgodnie z zatwierdzonym zakresem, prowadzi okresowe przeglądy uprawnień, dba o poprawność i kompletność danych, stanowi pierwszą linię wsparcia merytorycznego dla użytkowników, zgłasza błędy i potrzeby zmian, uczestniczy w testach akceptacyjnych.	Nie decyduje samodzielnie o przyznaniu dostępu poza zakresem zatwierdzonym przez właściciela biznesowego; nie odpowiada za kopie zapasowe, aktualizacje i bezpieczeństwo techniczne.
Administrator techniczny (administrator systemu / infrastruktury)	Pracownik komórki IT albo personel Wykonawcy utrzymującego system. Odpowiada za warstwę techniczną: instalację i konfigurację, aktualizacje i zarządzanie podatnościami, kopie zapasowe wraz z testami odtwarzania, monitorowanie dostępności i wydajności, rejestrowanie i przechowywanie logów, techniczne wykonanie nadania i odebrania uprawnień, zabezpieczenia techniczne (hartowanie, szyfrowanie, MFA), obsługę incydentów technicznych i dokumentację techniczną.	Nie decyduje o tym, komu przysługuje dostęp ani o zakresie przetwarzanych danych; dostęp do treści danych wyłącznie w zakresie niezbędnym do utrzymania, na podstawie upoważnienia i z rejestrowaniem czynności.

1.1.2. Wykonawca omówi ponadto zasadę rozdzielania obowiązków (zatwierdzający uprawnienia nie może ich technicznie nadawać), obowiązek udokumentowanego wyznaczenia tych ról dla każdego systemu, sposób postępowania przy zastępstwach i zmianie na stanowisku oraz współdziałanie tych ról z PBI, IOD i kierownictwem podczas obsługi incydentu i uruchomienia procedur ciągłości działania, w tym: decyzję właściciela biznesowego o priorytecie i trybie awaryjnym, weryfikację kompletności danych po odtworzeniu przez administratora merytorycznego oraz odtworzenie zasobu i raportowanie czasu odtworzenia przez administratora technicznego.

1.1.3. Wykonawca omówi podział systemów teleinformatycznych na systemy dziedzinowe (wspierające zadania jednej komórki merytorycznej, np. system kadrowo-płacowy, dziedzinowe bazy danych przyrodniczych) oraz systemy horyzontalne (obsługujące całą jednostkę, np. oprogramowanie antywirusowe / EDR, system kopii zapasowych, zabezpieczenia brzegowe, uwierzytelnianie wieloskładnikowe, system zgłoszeń), wraz z konsekwencjami tego podziału dla przypisania ról:

Kryterium	System dziedzinowy	System horyzontalny
Właściciel biznesowy	kierujący komórką merytoryczną, której zadanie ustawowe system realizuje	kierujący komórką właściwą do spraw informatyki (lub kierownictwo jednostki)
Definiowanie wymagań	komórka merytoryczna – zakres funkcjonalny, dane, zakres dostępu, wymagania ciągłości działania (RTO, RPO)	komórka IT – poziom i zakres zabezpieczenia, pokrycie, polityki techniczne
Skutek niedostępności	zatrzymanie procesu w jednej komórce	skutek dla całej jednostki, w tym dla systemów dziedzinowych
Rola komórki IT	administrator techniczny, opiniowanie rozwiązań, udział w odbiorach	właściciel biznesowy i administrator techniczny w jednej komórce – wymagana szczególna staranność w rozdzieleniu obowiązków
Finansowanie utrzymania i rozwoju	planowane przez komórkę merytoryczną będącą właścicielem; infrastruktura wspólna (serwery, kopie zapasowe, monitoring) pozostaje kosztem wspólnym jednostki	planowane przez komórkę IT, z uwzględnieniem odnowień po zakończeniu finansowania projektowego (np. ze środków KPO)

1.1.4. W odniesieniu do powyższego podziału Wykonawca omówi praktyczne konsekwencje dla uczestników, w szczególności: obowiązek udziału komórki IT w opiniowaniu zakupów oprogramowania i usług informatycznych niezależnie od komórki wnioskującej; uwzględnianie w planowaniu kosztu całkowitego posiadania systemu (licencje, wsparcie producenta, zasoby infrastrukturalne, kopie zapasowe, pracochłonność administracji technicznej); powiązanie deklarowanych parametrów ciągłości działania (RTO, RPO) z kosztem ich zapewnienia, ponoszonym w ramach planu finansowego właściciela biznesowego; konieczność zaplanowania odnowienia licencji i usług nabytych ze środków projektowych po zakończeniu okresu finansowania; prowadzenie rejestru systemów z przypisanym właścicielem biznesowym, administratorem merytorycznym i administratorem technicznym.

1.2. Blok II – NIS2 / UoKSC: ramy prawne i odpowiedzialność

- 1) wymagania dyrektywy NIS2 oraz krajowe wymagania wynikające z UoKSC;
- 2) omówienie roli GDOŚ i RDOŚ w świetle nowelizacji przepisów;
- 3) odpowiedzialność kadry kierowniczej;
- 4) obowiązki raportowe i dokumentacyjne.

1.3. Blok III – bezpieczne wykorzystanie AI w urzędzie

- 1) ryzyka związane z modelami LLM i generatywną AI, w tym wyciek danych;
- 2) zjawisko shadow AI i jego konsekwencje dla podmiotu publicznego;
- 3) rozpoznawanie materiałów typu deepfake;
- 4) bezpieczne promptowanie i dobre praktyki wykorzystania AI w urzędzie.

1.4. Blok IV – ciągłość działania

- 1) miejsce zarządzania ciągłością działania w SZBI oraz w wymaganiach UoKSC i KRI; podstawowe pojęcia zgodnie z normą PN-EN ISO 22301;
- 2) plan ciągłości działania (PCD) oraz plan odtworzenia po awarii (DRP) – struktura dokumentów, role, parametry RTO i RPO, zasoby krytyczne;
- 3) postępowanie pracownika w przypadku niedostępności systemów teleinformatycznych – tryb awaryjny pracy, obieg dokumentów, komunikacja zastępcza;
- 4) rola PBI i komórki IT w uruchomieniu, koordynowaniu i zakończeniu działań w ramach PCD, w tym decyzja o odtworzeniu danych z kopii zapasowych;
- 5) rola kierownictwa w zatwierdzaniu PCD, decyzjach o priorytetach odtwarzania oraz komunikacji na zewnątrz urzędu;
- 6) testowanie planów ciągłości działania, dokumentowanie testów i wykorzystanie wniosków do doskonalenia SZBI.

1.5. Blok V – warsztat / case study oraz test wiedzy

- 1) analiza realnych zagrożeń dedykowanych dla administracji publicznej;
- 2) ćwiczenie / symulacja incydentu (np. scenariusz ransomware) obejmujące zarówno reakcję na incydent, jak i uruchomienie procedur ciągłości działania, z wyraźnym podziałem ról pomiędzy pracownika, PBI, komórkę IT i kierownictwo;
- 3) omówienie podjętych decyzji operacyjnych i popełnionych błędów;
- 4) test wiedzy (quiz) na zakończenie Szkolenia wraz z omówieniem wyników i rekomendacjami końcowymi.

1.6. Szczegółowa agenda Szkolenia, z podziałem na godziny i bloki tematyczne, zostanie uzgodniona z Zamawiającym i podlega jego akceptacji na zasadach określonych w pkt 2.4. Zamawiający wymaga, aby zagadnienia dotyczące podziału ról (pracownik – PBI – komórka IT – kierownictwo) były omawiane w odniesieniu do dokumentacji SZBI obowiązującej u Zamawiającego, przekazanej Wykonawcy na etapie uzgadniania programu.

2. Wymagania ogólne dla realizacji Szkoleń

2.1. Wykonawca jest zobowiązany do uwzględnienia w ramach realizacji Przedmiotu zamówienia wymogów m.in. norm i przepisów:

- 1) PN-EN ISO/IEC 27001 oraz PN-EN ISO 22301;
- 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. (NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80);
- 6) Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;

- 7) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji);
- 8) innych właściwych przepisów prawa powszechnie obowiązującego, w szczególności z zakresu bezpieczeństwa informacji, ochrony danych osobowych oraz cyberbezpieczeństwa.
- 2.2. Szkolenia stacjonarne realizowane będą w siedzibie Zamawiającego. Salę szkoleniową wraz z wyposażeniem multimedialnym zapewnia Zamawiający.
- 2.3. Szkolenia w formie online realizowane będą na platformie Wykonawcy. Dostęp do platformy dla osoby prowadzącej Szkolenie oraz dla uczestników zapewnia Wykonawca. Platforma musi umożliwiać udział co najmniej 80 uczestników jednocześnie, zadawanie pytań oraz wygenerowanie raportu potwierdzającego uczestnictwo.
- 2.4. Wykonawca opracuje i przekaze Zamawiającemu do akceptacji, najpóźniej na 5 dni roboczych przed rozpoczęciem pierwszego Szkolenia: materiały szkoleniowe, szczegółowy program i harmonogram Szkolenia oraz wzór imiennego certyfikatu. Zamawiający w terminie 2 dni roboczych przekaze informację o akceptacji albo zgłosi uwagi, które Wykonawca zobowiązany będzie uwzględnić i przekazać poprawione dokumenty nie później niż na 2 dni robocze przed rozpoczęciem pierwszego Szkolenia.
- 2.5. Wykonawca wystawi uczestnikom imienne certyfikaty ukończenia Szkolenia, zawierające co najmniej: imię i nazwisko uczestnika, nazwę Szkolenia i zakres tematyczny, datę, miejsce/tryb, liczbę godzin, dane Wykonawcy i osoby prowadzącej oraz podstawę wydania. Przed wystawieniem certyfikatów Wykonawca przekaze Zamawiającemu do akceptacji próbkę certyfikatu w formacie PDF.
- 2.6. Wykonawca zapewni prowadzenie listy obecności (Szkolenia stacjonarne) oraz przekaze potwierdzenie uczestnictwa (Szkolenia online – raport z platformy), a także sporządzi raport poszkoleniowy zawierający daty, liczbę uczestników oraz agendę Szkoleń.
- 2.7. Zamawiający wymaga, aby wymiana informacji drogą elektroniczną odbywała się w sposób gwarantujący poufność przekazywanych danych i dokumentów. Dane osobowe uczestników przekazywane Wykonawcy (imię i nazwisko, miejsce pracy, służbowy adres e-mail) przesyłane są w formie zaszyfrowanych archiwów (standard AES-256, format .zip lub .7z), a hasła przekazywane są odrębnym kanałem komunikacji; zabrania się przysyłania hasła w tej samej wiadomości e-mail, w której znajduje się zaszyfrowany załącznik.
- 2.8. Wykonawca ponosi pełną odpowiedzialność za bezpieczeństwo danych przekazanych mu w celu realizacji Przedmiotu zamówienia oraz zobowiązany jest do ich usunięcia niezwłocznie po zakończeniu realizacji Przedmiotu zamówienia.
- 2.9. Wszystkie dokumenty wytworzone w trakcie realizacji Przedmiotu zamówienia muszą zostać przekazane w formatach edytowalnych (np. .docx, .pptx, .xlsx) oraz w formacie .pdf, a także muszą zostać odpowiednio oznaczone zgodnie z Księgą identyfikacji i wizualizacji Krajowego Planu Odbudowy oraz Strategią promocji i informacji KPO. Wytyczne oraz wzory dokumentów dostępne są pod adresem: <https://www.kpo.gov.pl/strony/o-kpo/dla-instytucji/dokumenty/strategia-promocji-i-informacji-kpo/> oraz <https://www.gov.pl/web/cppc/cyberbezpieczny-rzad> – zakładka „Materiały informacyjno-promocyjne”. Oznaczenie powinno być widoczne na dokumentach elektronicznych, w tym na prezentacji tytułowej i stronie tytułowej materiałów PDF oraz na certyfikatach, w sposób czytelny, zapewniający identyfikację dokumentu jako elementu realizacji projektu KPO.

- 2.10. Całość materiałów szkoleniowych oraz dokumentacji musi zostać opracowana w języku polskim, w sposób zwięzły i przystępny dla osób niebędących specjalistami IT.

3. Wymagania dotyczące kadry

- 3.1. Zamawiający wymaga, aby Szkolenia zostały przeprowadzone przez trenera, który spełnia łącznie następujące warunki:
- 1) posiada certyfikat Audytora Wiodącego SZBI wg normy PN-EN ISO/IEC 27001 wydany przez akredytowaną jednostkę certyfikującą (np. BSI, TÜV, PECB, IRCA) albo 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), np. CISA, CISM, CISSP, CGEIT;
 - 2) w okresie ostatnich 2 lat przed wszczęciem postępowania przeprowadził co najmniej 3 szkolenia z zakresu cyberbezpieczeństwa lub SZBI dla podmiotów publicznych.
- 3.2. Wykonawca po podpisaniu umowy przekaze Zamawiającemu dane osoby skierowanej do realizacji zamówienia.
- 3.3. Zamawiający wymaga zachowania ciągłości prac realizowanych przez trenera, o którym mowa w pkt 3.1. Zmiana trenera wymaga uprzedniej zgody Zamawiającego oraz wykazania, że osoba zastępująca spełnia warunki określone w pkt 3.1.
- 3.4. Wykonawca, a także osoby uczestniczące w realizacji Przedmiotu zamówienia, zobowiązane będą do złożenia oświadczenia o dochowaniu poufności w zakresie informacji pozyskanych w toku realizacji Przedmiotu zamówienia, przez okres obowiązywania umowy oraz przez 5 lat po jej rozwiązaniu lub wygaśnięciu.

4. Produkty Przedmiotu zamówienia i odbiór

- 4.1. Produktami Przedmiotu zamówienia są:
- 1) przeprowadzone Szkolenia – 5 sesji zgodnie z pkt 1.1. części II;
 - 2) materiały szkoleniowe w języku polskim w formie elektronicznej (PDF oraz format edytowalny);
 - 3) imienne certyfikaty ukończenia Szkolenia dla uczestników;
 - 4) listy obecności oraz potwierdzenia uczestnictwa;
 - 5) raport poszkoleniowy obejmujący daty, liczbę uczestników oraz agendę Szkoleń.
- 4.2. Potwierdzeniem należytego wykonania Przedmiotu zamówienia jest protokół odbioru podpisany przez Zamawiającego w terminie 5 dni roboczych od zakończenia ostatniego Szkolenia, po przekazaniu przez Wykonawcę kompletu produktów, o których mowa w pkt 4.1.

5. Prawa autorskie

- 5.1. Z dniem zaakceptowania przez Zamawiającego materiałów szkoleniowych Wykonawca przenosi na Zamawiającego, w ramach przysługującego wynagrodzenia, autorskie prawa majątkowe do tych materiałów na polach eksploatacji określonych w projektowanych postanowieniach umowy, w tym w zakresie utrwalania i zwielokrotniania, rozpowszechniania, publikowania w intranecie Zamawiającego oraz wykorzystywania w działalności statutowej Zamawiającego i JP.
- 5.2. Wykonawca przenosi na Zamawiającego prawo zezwalania na wykonywanie zależnych praw autorskich do materiałów szkoleniowych oraz zobowiązuje się do niewykonywania autorskich praw osobistych w stosunku do Zamawiającego.