załącznik nr 3 do Umowy cz.2

Szczegółowy Opis Przedmiotu Zamówienia

Nazwa: **Szkolenie administratorów systemów informatycznych z AI realizowane na rzecz Rządowego Centrum Bezpieczeństwa.**

Przedmiot zamówienia obejmuje szkolenie z zarządzania ryzykiem i bezpieczeństwo AI w sektorze publicznym

- czas trwania (1dzień);
- poziom (średnio zaawansowany);
- tryb (online).

Szkolenie powinno obejmować co najmniej następujące zagadnienia:

1.1. Zrozumienie specyficznego ryzyka związanego z AI w kontekście rządowym:
- jak ryzyko AI różni się od tradycyjnego ryzyka IT i danych;
- kategorie ryzyka AI: techniczne, operacyjne, reputacyjne i etyczne;
- odpowiedzialność publiczna i postrzeganie ryzyka w rządzie.

1.2. Ramy zarządzania ryzykiem AI:
- ramy Zarządzania Ryzykiem AI NIST (AI RMF);
- ISO/IEC 42001:2023 — Standard Systemu Zarządzania AI;
- inne wytyczne sektorowe i międzynarodowe (np. OECD, UNESCO).

1.3. Zagrożenia bezpieczeństwa dla systemów AI:
- wrogie dane wejściowe, zatruwanie danych i inwersja modelu;
- ujawnienie wrażliwych danych treningowych;
- ryzyka związane z łańcuchem dostaw i modelami stron trzecich.

1.4. Zarządzanie, audyt i kontrola:
- mechanizmy odpowiedzialności z udziałem człowieka;
- audytowalne AI: dokumentacja, wersjonowanie i interpretowalność;
- kontrole wewnętrzne, role nadzorcze i punkty kontrolne zgodności.

1.5. Ocena ryzyka i planowanie działań zaradczych:
- tworzenie rejestrów ryzyka dla przypadków użycia AI;
- współpraca z zespołami ds. zamówień, prawnymi i projektowania usług;
- przeprowadzanie ocen przed wdrożeniem i po wdrożeniu.
- Reagowanie na incydenty i odporność sektora publicznego:
  - ✓ reagowanie na incydenty i naruszenia związane z AI;
  - ✓ komunikacja z interesariuszami i społeczeństwem;
  - ✓ wdrażanie praktyk zarządzania ryzykiem AI w podręcznikach cyberbezpieczeństwa.

2. Pozostałe wymagania dotyczące szkolenia;
- liczba osób wskazanych do szkolenie – min. 1 osoba;

- poziom zaawansowania – średni;
- tryb (online).

2.1. Wykonawca zapewni:
- materiały szkoleniowe w języku polskim lub angielskim;
- instrukcje do laboratoriów;
- prezentacje;
- dokumentację techniczną;
- dostęp do środowiska laboratoryjnego na czas szkolenia (jeżeli tematy szkolenia tego wymagają);
- indywidualne środowisko laboratoryjne dla każdego uczestnika szkolenia (jeżeli tematy szkolenia tego wymagają);

2.2. Termin szkolenia – po uzgodnieniu z Zamawiającym;

2.3. Forma szkolenia – online, obejmująca ćwiczenia praktycznie na środowisku testowym Wykonawcy (jeżeli takie są wymagane przez Zamawiającego);

2.4. Po zakończeniu szkolenia uczestnik otrzyma imienny certyfikat potwierdzający ukończenie szkolenia z zakresu objętego szkoleniem;

2.5. Zamawiający nie wymaga szkolenia autoryzowanego;