Załącznik nr 1.5 do SWZ
Nr wewn. post. 52/25

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA
USŁUGA SPOŁECZNA

1) Opis przedmiotu zamówienia

Certyfikowane specjalistyczne szkolenie online (ISC)² CISSP (Certified Information Systems Security) dla 7 specjalistów i praktyków z zakresu informatyki śledczej oraz Cyberbezpieczeństwa z Zarządu w Radomiu Centralnego Biura Zwalczania Cyberprzestępczości w ramach projektu nr FBWP.03.01-IZ.00-0002/24 pn. „CyberShield – wzmocnienie kompetencji Policji w zakresie zwalczania cyberprzestępczości" dofinansowywanego ze środków Funduszu Bezpieczeństwa Wewnętrznego na lata 2021-2027.

2) Szczegóły szkolenia

Przeprowadzenie szkolenia przygotowującego do egzaminu **(ISC)² CISSP - Certified Information Systems Security Professional w wersji najbardziej aktualnej na dzień rozpoczęcia** szkolenia wraz z voucherem na egzamin certyfikacyjny (ISC)² CISSP ważnym min. 3 miesiące po zakończeniu szkolenia. Celem szkolenia CISSP (Certified Information Systems Security Professional) jest przygotowanie uczestników do zdobycia certyfikacji w dziedzinie bezpieczeństwa informacji. Szkolenie umożliwia zdobycie wiedzy i umiejętności niezbędnych do projektowania, wdrażania i zarządzania kompleksowymi systemami bezpieczeństwa w organizacjach zgodnie z międzynarodowymi standardami.

3) Odbiorcy szkolenia

Szkolenie przeznaczone jest dla 7 specjalistów i praktyków z zakresu informatyki śledczej oraz Cyberbezpieczeństwa z Zarządu w Radomiu Centralnego Biura Zwalczania Cyberprzestepczości. Uczestnikami szkolenia będzie łącznie 7 osób w ramach jednej grupy szkoleniowej.

4) Wymagania ogólne dotyczące realizacji szkolenia

a) Szkolenie musi zostać przeprowadzone w oparciu o autoryzowane materiały szkoleniowe (ISC)² CISSP
b) Szkolenie musi być zgodne merytorycznie z oficjalnym seminarium CISSP: „Official ISC2 CBK Training Seminar for the CISSP (Certified Information Systems Security Professional)", a program szkolenia w pełni zgodny z aktualnie obowiązującym kanonem wiedzy wymaganej w czasie egzaminu CISSP.
c) Szkolenie musi być przeprowadzone przez autoryzowanego instruktora ISC2 posiadającego poświadczenia trenerskie wystawione przez ISC2 oraz certyfikat CISSP.
d) Wykonawca szkolenia zapewni dla każdego uczestnika dostęp do platformy szkoleniowej do komunikacji audio/video dającej możliwość przeprowadzenia na żywo, przy użyciu sieci Internet, zajęć teoretycznych i praktycznych z możliwością udostępniania obrazu z pulpitu zarówno przez prowadzących, jak i uczestników. Indywidualne stanowiska robocze (komputery kursantów) zostaną zapewnione przez Zamawiającego.
e) Wykonawca przeprowadzi szkolenie w języku polskim.
f) Wykonawca jest Oficjalnym Partnerem Szkoleniowym (ISC)² – Authorized Training Partner (ATP) *lub* posiada pisemne upoważnienie (ISC)² do realizacji kursu „Official CBK Training Seminar for CISSP".
g) Wykonawca zrealizuje szkolenie w terminie 2 miesięcy od daty zawarcia umowy.
h) Wykonawca w uzgodnieniu z Zamawiającym wyznaczy termin realizacji szkolenia.
i) Szkolenie musi obejmować 5 kolejnych dni roboczych.
j) Każdy dzień szkoleniowy to 7 godzin zegarowych. Dokładny harmonogram dzienny dla poszczególnych modułów zostanie uzgodniony z Wykonawcą w ramach kontaktów roboczych.
k) Wykonawca zapewni akredytowane materiały szkoleniowe (ISC)² CISSP odpowiednie dla tematyki szkolenia, dla każdego z uczestników szkolenia. Materiały szkoleniowe muszą być przygotowane w języku polskim lub angielskim. Materiały szkoleniowe mogą być w formie papierowej lub w formie elektronicznej. Koszty opracowania, powielenia i transportu materiałów szkoleniowych ponosi Wykonawca. Materiały muszą być zgodne z aktualnie obowiązującym kanonem wiedzy wymaganej w czasie egzaminu CISSP. Wykonawca ponosi pełną odpowiedzialność za zgodność merytoryczną oraz aktualność przekazywanych danych/informacji w materiałach szkoleniowych.
l) Uczestnicy otrzymają imienne certyfikaty ukończenia szkolenia, zawierające informacje o podmiocie realizującym szkolenie, danymi trenera/trenerów oraz potwierdzenie ukończenia kursu przygotowującego do certyfikacji (ISC)² CISSP.
m) Certyfikaty, o których mowa powyżej, muszą zawierać informację o ukończeniu szkolenia przygotowującego do certyfikacji (ISC)² CISSP oraz oznaczenia wskazujące na finansowanie ze środków FBW w ramach Projektu (Zamawiający przekaże Wykonawcy niezbędne pliki graficzne).

n) Po zakończeniu szkolenia Wykonawca zobowiązuje się do przekazania uczestnikom szkolenia imiennych voucherów na egzaminy certyfikacyjne (ISC)² CISSP w wersji najbardziej aktualnej na dzień rozpoczęcia szkolenia.
o) **Wykonawca dysponuje platformą on-line wykorzystywaną przez (ISC)²** (np. Zoom-ISC², Adobe Connect) lub równoważną, zapewniającą:
• audio/wideo HD, czat, dwustronne udostępnianie ekranu;
• dostępność, SLA ≥ 99 %

5) Zakres merytoryczny szkolenia

Program szkolenia musi obejmować osiem kluczowych domen wiedzy, zgodnych z Common Body of Knowledge (CBK) opracowanym przez (ISC)²:

- Zarządzanie bezpieczeństwem i ryzykiem (Security and Risk Management)
  - Zasady zarządzania bezpieczeństwem, zgodność z regulacjami prawnymi i normami.
  - Zarządzanie ryzykiem, modelowanie zagrożeń i zarządzanie łańcuchem dostaw.
- Bezpieczeństwo zasobów (Asset Security)
  - Klasyfikacja informacji i zasobów, kontrola cyklu życia danych oraz wymogi dotyczące ich ochrony.
- Architektura i inżynieria bezpieczeństwa (Security Architecture and Engineering)
  - Projektowanie bezpiecznych systemów, kryptografia, modele oceny bezpieczeństwa oraz ochrona infrastruktury.
- Bezpieczeństwo komunikacji i sieci (Communication and Network Security)
  - Projektowanie bezpiecznych architektur sieciowych, ochrona kanałów komunikacyjnych oraz komponentów sieciowych.
- Zarządzanie tożsamością i dostępem (Identity and Access Management)
  - Mechanizmy uwierzytelniania, zarządzanie tożsamościami oraz kontrola dostępu.
- Ocena i testowanie bezpieczeństwa (Security Assessment and Testing)
  - Testowanie kontroli bezpieczeństwa, audyty oraz analiza wyników testów.
- Operacje związane z bezpieczeństwem (Security Operations)
  - Zarządzanie incydentami, procesy odzyskiwania po awarii oraz monitorowanie operacyjne.
- Bezpieczeństwo w cyklu życia oprogramowania (Software Development Security)
  - Integracja zasad bezpieczeństwa w procesach tworzenia oprogramowania oraz ocena wpływu zabezpieczeń na aplikacje.