Załącznik Nr 1
do zapytania ofertowego nr 10/2019

I. Dane Zamawiającego

Collegium Civitas
Plac Defilad 1, PKiN p. XII
00-901 Warszawa
NIP 525-20-83-784, REGON 012769984

II. Doświadczenie

Osoby składające ofertę powinny spełniać co najmniej poniższe kryteria:

Część 1

- posiadać minimum tytuł magistra;
- ekspert w ramach dziedziny, w której prowadzone są zajęcia;
- doświadczenie w obszarze IT i cyberbezpieczeństwa w administracji publicznej i/lub sektorze prywatnym;
- co najmniej 3 lata doświadczenia dydaktycznego (prowadzenie zajęć w obszarze tematycznym związanym z cyberbezpieczeństwem i/lub bezpieczeństwem informacyjnym).

Część 2

- posiadać minimum tytuł doktora;
- ekspert w ramach dziedziny, w której prowadzone są zajęcia;
- doświadczenie w obszarze cyberbezpieczeńststwa w administracji publicznej i/lub sektorze prywatnym;
- co najmniej 3 lata doświadczenia dydaktycznego (prowadzenie zajęć dydaktycznych i/lub szkoleń w obszarze tematycznym związanym z cyberbezpieczeństwem i/lub bezpieczeństwem informacyjnym).

Część 3

- posiadać minimum tytuł doktora;
- ekspert w ramach dziedziny, w której prowadzone są zajęcia;
- doświadczenie w obszarze cyberbezpieczeńststwa w administracji publicznej i/lub sektorze prywatnym;

- co najmniej 3 lata doświadczenia dydaktycznego (prowadzenie zajęć dydaktycznych i/lub szkoleń w obszarze tematycznym związanym z cyberbezpieczeństwem i/lub bezpieczeństwem informacyjnym).

Część 4

- posiadać minimum tytuł doktora;
- ekspert w ramach dziedziny, w której prowadzone są zajęcia;
- doświadczenie w obszarze cyberbezpieczeńststwa w administracji publicznej i/lub sektorze prywatnym;
- co najmniej 3 lata doświadczenia dydaktycznego (prowadzenie zajęć dydaktycznych i/lub szkoleń w obszarze tematycznym związanym z cyberbezpieczeństwem i/lub bezpieczeństwem informacyjnym).

Część 5

- posiadać minimum tytuł magistra;
- ekspert w ramach dziedziny, w której prowadzone są zajęcia;
- doświadczenie w obszarze IT i cyberbezpieczeńststwa w administracji publicznej i/lub sektorze prywatnym;
- co najmniej 3 lata doświadczenia dydaktycznego (prowadzenie zajęć w obszarze tematycznym związanym z cyberbezpieczeństwm i/lub bezpieczeństwem informacyjnym)

Doświadczenie oraz posiadane kwalifikacje należy opisać w załączniku nr 4 do zapytania ofertowego, a na potwierdzenie przedłożyć dokumenty potwierdzające kwalifikacje zawodowe/referencje.

III. Opis przedmiotu zamówienia

Przedmiot zamówienia został podzielony w następujący sposób:

Część 1

Nazwa kierunku/stopień	Tryb studiów	Nazwa specjalności	Nazwa przedmiotu	Ilość godzin	Ogólny zakres merytoryczny
Stosunki międzynarodowe, I stopień	stacjonarny	Cyberbezpieczeństwo	Bezpieczeństwo systemów teleinformatycznych	30h	Przedmiot powinien obejmować treści dotyczące kompleksowego podejścia do zagadnień związanych z ochroną systemów teleinformatycznych w podziale na: – bezpieczeństwo aplikacji, – bezpieczeństwo kodu na podstawie metodyki OWASP, – bezpieczeństwo sieci teleinformatycznych, – bezpieczeństwo części serwerowej, – bezpieczeństwo sieci bezprzewodowych, VPN – bezpieczeństwo systemów operacyjnych, – szacowanie ryzyk, – planowanie strategii działania, – wstęp do kryptografii.
	niestacjonarny			20h	

Część 2

Nazwa kierunku/stopień	Tryb studiów	Nazwa specjalności	Nazwa przedmiotu	Ilość godzin	Ogólny zakres merytoryczny
Stosunki międzynarodowe, I stopień	stacjonarny	Cyberbezpieczeństwo	Cyberprzestrzeń jako pole konfliktu	30h	Zajęcia obejmować powinny przybliżenie problematyki zagrożeń w cyberprzestrzeni, możliwych taktyk i strategii działania państwa w tym obszarze: – definiowanie walki informacyjnej, – definiowanie cyberprzestrzeni jako płaszczyzny konfliktu,

	niestacjonarny			20h	– operacje psychologiczne w cyberprzestrzeni i propaganda w cyberprzestrzeni, – cyber-wojna i net-wojna, – konflikt sieciowy, konflikt "zdigitalizowany", – cyberprzestępczość: formy i metody działania przestępców, – ocena zagrożeń dla bezpieczeństwa państwa w cyberprzestrzeni, – cyberterroryzm M. Terlikowski, – narodowe i międzynarodowe strategie cyber-bezpieczeństwa, – case studies

Część 3

Nazwa kierunku/stopień	Tryb studiów	Nazwa specjalności	Nazwa przedmiotu	Ilość godzin	Ogólny zakres merytoryczny
Stosunki międzynarodowe, I stopień	stacjonarny	Cyberbezpieczeństwo	Walka informacyjna	30h	Zajęcia powinny pozwolić na zapoznanie studentów z podstawami funkcjonowania różnorodnych podmiotów w środowisku informacyjnym w warunkach walki informacyjnej: – walka informacyjna – definiowanie, – metody i formy walki informacyjnej, – zasoby informacyjne jako zasoby strategiczne, – rola zasobów informacyjnych w procesie decyzyjnym, – wywiad gospodarczy, – manipulacja, dezinformacja, propaganda, – psychomanipulacja i socjotechnika, – edukacja i świadomość społeczna w walce informacyjnej, – zagrożenia dla procesów demokratycznych.
	niestacjonarny			20h	

Część 4

Nazwa kierunku/stopień	Tryb studiów	Nazwa specjalności	Nazwa przedmiotu	Ilość godzin	Ogólny zakres merytoryczny
Stosunki międzynarodowe, I stopień	stacjonarny	Cyberbezpieczeństwo	Projektowanie procedur bezpieczeństwa	30h	Przedmiot powinien obejmować treści dotyczące praktycznych aspektów tworzenia rozwiązań regulacyjnych w obszarze bezpieczeństwa informacyjnego i cyberbezpieczeństwa: – procedura – definicja, praktyczne zastosowania, – projektowanie algorytmów postępowania, – testowanie i wdrażanie procedur, – dobre praktyki w obszarze procedur bezpieczeństwa informacyjnego i cyberbezpieczeństwa, – analiza zagrożeń oraz słabych punktów systemu, – zasady formułujące prawidłowy dostęp i zarządzanie informacjami w sieci, – metody postępowania podczas naruszenia bezpieczeństwa, – instruktaż pracowników mechanizmy autoryzacji i uwierzytelnienia.
	niestacjonarny			20h	

Część 5

Nazwa kierunku/stopień	Tryb studiów	Nazwa specjalności	Nazwa przedmiotu	Ilość godzin	Ogólny zakres merytoryczny
Stosunki międzynarodowe, I stopień	stacjonarny	Cyberbezpieczeństwo	Audyt systemów teleinformatycznych	30h	Przedmiot powinien pozwolić na zapoznanie studentów z rozwiązaniami w zakresie audytu rozwiązań teleinformatycznych: – audyt rozwiązań teleinformatycznych w oparciu o normy z rodziny ISO 27001 w obszarach: a. polityka bezpieczeństwa; b. organizacja bezpieczeństwa informacji; c. zarządzanie aktywami; d. bezpieczeństwo zasobów ludzkich; e. bezpieczeństwo fizyczne i środowiskowe; f. zarządzanie systemami i sieciami;

	niestacjonarny			20h	g. kontrola dostępu; h. zarządzanie ciągłością działania; i. pozyskiwanie, rozwój i utrzymanie systemów informatycznych; j. zarządzanie incydentami związanymi z bezpieczeństwem informacji; k. zgodność z wymaganiami prawnymi i własnymi standardami. – proces zbierania i ewidencjonowania dowodów w celu stwierdzenia zgodności z określonymi normami – sporządzanie i zawartość raportu z audytu.

IV. Wymagania odnośnie standardu prowadzonych zajęć

1. Opracowanie sylabusów do zajęć, które będą prowadzone przez Oferenta – według standardu Zamawiającego.
2. Przeprowadzenie zajęć w ramach semestru letniego w maksymalnym wymiarze 30h na studiach stacjonarnych i 20h na studiach niestacjonarnych.
3. Prowadzenie i weryfikacja list obecności studentów na zajęciach – według wzorów Zamawiającego.
4. Przekazanie po zrealizowaniu zajęć uzupełnionych list obecności na zajęciach, jednak nie później w terminie 14 dni od zakończenia zajęć.
5. Zorganizowanie i przeprowadzenie egzaminu zaliczającego prowadzony przedmiot oraz uzupełnienie wszelkiej dokumentacji z tym związanej.
6. Informowania uczestników zajęć, iż zajęcia są współfinansowane ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.
7. Umieszczania na prezentacjach/materiałach logotypów zgodnych z Wytycznymi w zakresie informacji i promocji programów operacyjnych polityki spójności na lata 2014-2020.
8. Umożliwienie przeprowadzenia kontroli zajęć zarówno przez przedstawiciela Zamawiającego, jak również przez instytucje zarządzające programem w ramach którego dofinansowano projekt.