Załącznik Nr 1
do zapytania ofertowego nr 4/2020

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 – na prowadzenie zajęć z przedmiotu *Struktury sieciowe i jako podstawa nowego paradygmatu bezpieczeństwa*

- posiadać minimum tytuł magistra;
- ekspert w ramach dziedziny, w której prowadzone są zajęcia;
- doświadczenie w bezpieczeństwa pozamilitarnego, w tym zwłaszcza bezpieczeństwa informacyjnego w administracji publicznej i/lub sektorze prywatnym;
- co najmniej 5 lat doświadczenia dydaktycznego (prowadzenie zajęć w obszarze tematycznym związanym z cyberbezpieczeństem i/lub bezpieczeństwem informacyjnym);
- umiejętność prowadzenia zajęć w trybie zdalnym z wykorzystaniem Microsoft Teams lub innych platform edukacyjnych.

Część 2 - na prowadzenie zajęć z przedmiotu *Ochrona danych osobowych uwarunkowania prawne i techniczne*

- 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);
- umiejętność prowadzenia zajęć w trybie zdalnym z wykorzystaniem Microsoft Teams lub innych platform edukacyjnych.

Część 3 - na prowadzenie zajęć z przedmiotu *Cyberprzestępczość*

- posiadać minimum tytuł magistra;

- ekspert w ramach dziedziny, w której prowadzone są zajęcia;
- doświadczenie w obszarze cyberbezpieczeństwa w administracji publicznej i/lub sektorze prywatnym;
- co najmniej 5 lat doświadczenia dydaktycznego (prowadzenie zajęć dydaktycznych i/lub szkoleń w obszarze tematycznym związanym z cyberbezpieczeństwem i/lub bezpieczeństwem informacyjnym);
- umiejętność prowadzenia zajęć w trybie zdalnym z wykorzystaniem Microsoft Teams lub innych platform edukacyjnych.

Część 4 – na prowadzenie zajęć z przedmiotu *Informatyka śledcza*

- posiadać minimum tytuł magistra;
- ekspert w ramach dziedziny, w której prowadzone są zajęcia;
- doświadczenie w obszarze cyberbezpieczeństwa w administracji publicznej i/lub służbach bezpieczeństwa i porządku publicznego;
- co najmniej 3 lata doświadczenia dydaktycznego (prowadzenie zajęć dydaktycznych i/lub szkoleń w obszarze tematycznym związanym z cyberbezpieczeństwem i/lub informatyką śledczą);
- umiejętność prowadzenia zajęć w trybie zdalnym z wykorzystaniem Microsoft Teams lub innych platform edukacyjnych.

Część 5 – na prowadzenie zajęć z przedmiotu *System zabezpieczeń pomieszczeń i urządzeń*

- 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;
- doświadczenie we wdrażaniu i realizowaniu rozwiązań w zakresie zabezpieczania zasobów informacyjnych instytucji;
- Umiejętność prowadzenia zajęć w trybie zdalnym z wykorzystaniem Microsoft Teams lub innych platform edukacyjnych.

Część 6 - na prowadzeniezajęć z przedmiotu *Walka o wizerunek w środowisku Internetu*

- posiadać minimum tytuł doktora;
- ekspert w ramach dziedziny, w której prowadzone są zajęcia;
- doświadczenie w obszarze cyberbezpieczeństwa w administracji publicznej i/lub sektorze prywatnym;
- co najmniej 5 lat doświadczenia dydaktycznego (prowadzenie zajęć dydaktycznych i/lub szkoleń w obszarze tematycznym związanym z cyberbezpieczeństwem i/lub bezpieczeństwem informacyjnym).
- Umiejętność prowadzenia zajęć w trybie zdalnym z wykorzystaniem Microsoft Teams lub innych platform edukacyjnych

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	Struktury sieciowe jako podstawa nowego paradygmatu bezpieczeństwa	30h	Przedmiot powinien pozwolić na zapoznanie studentów z zagadnieniami związanymi ze strukturami sieciowymi jako podstawą nowego paradygmatu bezpieczeństwa: – sieciowy paradygmat bezpieczeństwa narodowego, – środowisko bezpieczeństwa: szanse, wyzwania, zagrożenia, ryzyko, – pojęcie sieci: sieć jako struktura i środowisko działania, – analiza struktur sieciowych, – państwo jako węzeł sieci, – zdolności ofensywne i defensywne państwa w walce sieciowej.
	niestacjonarny			20h	

Część 2

Nazwa kierunku/stopień	Tryb studiów	Nazwa specjalności	Nazwa przedmiotu	Ilość godzin	Ogólny zakres merytoryczny
Stosunki międzynarodowe, I stopień	stacjonarny	Cyberbezpieczeństwo	Ochrona danych osobowych: uwarunkowania prawne i techniczne	30h	Przedmiot powinien obejmować treści dotyczące ochrony danych osobowych, jej uwarunkowań prawnych i technicznych: – pojęcie danych osobowych i rodzaje danych osobowych, – podstawy prawne ochrony danych osobowych, RODO, – zasady przetwarzania danych osobowych, – przetwarzanie danych wrażliwych, – obowiązki administratora danych osobowych, – uprawnienia osób, których dane osobowe są przetwarzane, – inspektor ochrony danych osobowych: status i uprawnienia, – ochrona integralności, poufności i dostępności danych, – organizacyjne i techniczne rozwiązania w zakresie ochrony danych osobowych.
	niestacjonarny			20h	

Część 3

Nazwa kierunku/stopisz	Tryb studiów	Nazwa specjalności	Nazwa przedmiotu	Ilość godzin	Ogólny zakres merytoryczny
Stosunki międzynarodowe, I stopień	stacjonarny	Cyberbezpieczeństwo	Cyberprzestępczość	30h	Przedmiot powinien obejmować treści dotyczące przestępczości w cyberprzestrzeni oraz prewencji i zwalczania jej: – przestępczość komputerowa, – przestępczość przeciwko poufności, integralności i dostępności danych,

	niestacjonarny			20h	– przestępczość w cyberprzestrzeni, – socjotechnika i manipulacja jako narzędzia sprawców przestępstw z wykorzystaniem komputerów, – przestępstwa związane z rozpowszechnianiem nielegalnych treści, – specyfika ścigania poszczególnych rodzajów przestępstw.

Część 4

Nazwa kierunku/stopień	Tryb studiów	Nazwa specjalności	Nazwa przedmiotu	Ilość godzin	Ogólny zakres merytoryczny
Stosunki międzynarodowe, I stopień	stacjonarny	Cyberbezpieczeństwo	Informatyka śledcza	30h	Zajęcia powinny pozwolić na zapoznanie studentów z podstawami informatyki śledczej, jej zadań, stosowanych rozwiązań oraz wykorzystywanych narzędzi: – wymogi prawne w postępowaniu dowodowym, – omówienie narzędzi i niezbędnego sprzętu, – wykorzystywanie bezpłatnych narzędzi w zbieraniu dowodów elektronicznych, – zabezpieczanie i analiza zawartości pamięci RAM, – zabezpieczanie i analiza zawartości elektronicznych nośników danych, odzyskiwanie usuniętych plików.
	niestacjonarny			20h	

Część 5

Nazwa kierunku/stopień	Tryb studiów	Nazwa specjalności	Nazwa przedmiotu	Ilość godzin	Ogólny zakres merytoryczny
Stosunki międzynarodowe, I stopień	stacjonarny	Cyberbezpieczeństwo	Systemy zabezpieczeń pomieszczeń i urządzeń	30h	Zajęcia obejmować powinny przybliżenie problematyki systemów zabezpieczeń pomieszczeń i urządzeń i ich roli w zapewnieniu bezpieczeństwa zasobów informacyjnych podmiotu:: – definiowanie bezpieczeństwa i form zabezpieczeń,

	niestacjonarny			20h	– zasady postępowania przy dostępie do danych jawnych i niejawnych, – zasady tworzenia podziału stref dostępu, – kradzież informacji: formy i metody działania przestępców, – stosowane formy systemów zabezpieczeń pomieszczeń i urządzeń, – ocena zagrożeń dostępu do informacji na konkretnym przykładzie.

Część 6

Nazwa kierunku/stopień	Tryb studiów	Nazwa specjalności	Nazwa przedmiotu	Ilość godzin	Ogólny zakres merytoryczny
Stosunki międzynarodowe, I stopień	stacjonarny	Cyberbezpieczeństwo	Walka o wizerunek w środowisku internetu	30h	Przedmiot powinien pozwolić na zapoznanie studentów zagadnieniami związanymi z ochroną wizerunku jednostki oraz instytucji w internecie: – charakterystyka internetu i mediów społecznościowych jako środowiska walki o wizerunek, – świadome budowanie wizerunku w internecie, – kreowanie wizerunku firmy w internecie, – networking w internecie, – zagrożenia dla wizerunku w internecie / kryzysy wizerunkowe, – zarządzaniem kryzysem marki / wizerunku, – ochrona prawna wizerunku.
	niestacjonarny			20h	

IV. Wymagania odnośnie standardu prowadzonych zajęć:

1. Opracowanie sylabusów do zajęć, które będą prowadzone przez Oferenta - według standardu Zamawiającego.
2. Przeprowadzenie zajęć w ramach specjalności będzie realizowane w formie zdalnej, w maksymalnym wymiarze 30 h na studiach stacjonarnych i w maksymalnym wymiarze 20 h na studiach niestacjonarnych.

3. Prowadzenie i weryfikacja list obecności studentów na zajęciach – według wzoru Zamawiającego.
4. Przekazanie po zrealizowaniu uzupełnionych list obecności na zajęciach, jednak nie później w terminie 14 dni od zakończenia.
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. Umieszczenia 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.