Możliwość dofinansowania

Studia podyplomowe_Bezpieczeństwo informacji i ochrona danych osobowych (online)

Numer usługi 2024/07/30/12546/2242256

4 100,00 PLN brutto
4 100,00 PLN netto
23,30 PLN brutto/h
23,30 PLN netto/h

Uniwersytet Ekonomiczny w Katowicach

★★★★☆

zdalna w czasie rzeczywistym
Studia podyplomowe
176 h
16.11.2024 do 30.06.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Studia skierowane są głównie do osób zajmujących się problematyką ochrony informacji i danych osobowych, a także do osób odpowiedzialnych w firmie za bezpieczeństwo, a więc: 1. osób wyznaczonych do wykonywania funkcji administratora bezpieczeństwa informacji czy administratora danych osobowych, 2. innych podmiotów mających w swej działalności do czynienia z danymi osobowymi, w celu podniesienia kwalifikacji, 3. absolwentów wyższych uczelni, wszystkich kierunków (szczególnie kierunki: prawo, administracja, zarządzanie, informatyka lub ekonomia), 4. osób, które zamierzają pełnić funkcje Inspektora ochrony danych osobowych, Menedżera bezpieczeństwa informacji lub Audytora SZBI, pracowników działów personalnych i IT w urzędach administracji rządowej i samorządowej. Studia podyplomowe są dedykowane również tym osobom, które myślą o przekwalifikowaniu się i pracy w działach związanych z ochroną danych osobowych.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	40
Data zakończenia rekrutacji	15-10-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	176

Podstawa uzyskania wpisu do BUR	art. 163 ust. 1 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (t.j. Dz. U. z 2023 r. poz. 742, z późn. zm.)
Zakres uprawnień	Studia podyplomowe

Cel

Cel edukacyjny

Głównym celem studiów jest przygotowanie uczestników do pełnienia kierowniczych funkcji w obszarze zarządzania bezpieczeństwem informacji i ochrony danych osobowych, zgodnie z nowym rozporządzeniem oraz zapoznanie uczestników ze standardami zarządzania bezpieczeństwem informacji. Ukończenie studiów pozwoli na zdobycie wiedzy umożliwiającej wykonywanie funkcji Managera Bezpieczeństwa Informacji lub Inspektora Ochrony Danych Osobowych oraz Audytora Systemu Zarządzania Bezpieczeństwem Informacji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
WIEDZA: - zna i rozumie w pogłębionym stopniu – wybrane fakty, obiekty i zjawiska z obszaru bezpieczeństwa informacji oraz ochrony danych osobowych oraz dotyczące ich metody i teorie wyjaśniające złożone zależności między nimi, stanowiące zaawansowaną wiedzę ogólną z zakresu nauki o zarządzaniu i jakości oraz z zakresu dyscyplin uzupełniających: ekonomii i finansów, matematyki i informatyki, komunikacji i nowych mediów tworzących podstawy teoretyczne, uporządkowaną i podbudowaną teoretycznie wiedzę obejmującą kluczowe zagadnienia oraz wybrane zagadnienia z zakresu zaawansowanej wiedzy szczegółowej – właściwe dla programu studiów na kierunku "Bezpieczeństwo informacji i ochrona danych osobowych"	Definiuje i charakteryzuje zagadnienia takie, jak: bezpieczeństwo informacji, dane osobowe i ich rodzaje, system zarządzania bezpieczeństwem informacji, norma ISO 27001, Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27.04.2016 (RODO), zakres roli, zadania inspektora ochrony danych osobowych, zgoda na przetwarzanie danych osobowych, dokumentacja z zakresu ochrony danych osobowych, polityka ochrony danych osobowych, norma ISO 22301, audyt, zarządzanie ryzykiem, norma ISO 31000, norma ISO 27005	Test teoretyczny
- zna i rozumie fundamentalne dylematy współczesnej cywilizacji oraz wynikające z nich koncepcje zarządzania, opisu i tworzenia relacji między kręgami kulturowymi, instytucjami i organizacjami w gospodarce w wymiarze lokalnym, regionalnym i międzynarodowym, które są istotne w procesie zapewniania bezpieczeństwa informacji i ochrony danych osobowych - zna i rozumie ekonomiczne, prawne, etyczne i inne uwarunkowania działalności zawodowej menedżerów bezpieczeństwa informacji, inspektora ochrony danych osobowych oraz audytora systemu zarządzania bezpieczeństwem informacji według normy ISO/IEC 27001 - zna i rozumie zasady bezpieczeństwa informacji i ochrony danych osobowych w różnych formach i rodzajach przedsiębiorczości	Definiuje i charakteryzuje zagadnienia takie, jak: prawo dot. ochrony danych osobowych, incydenty bezpieczeństwa, incydent naruszenia ochrony danych osobowych, zabezpieczenia i poziom bezpieczeństwa, komunikacja wielokulturowa, anonimizacja danych, sądy właściwe w sprawach dotyczących naruszenia ochrony danych osobowych, audyt i jego rodzaje w obszarze bezpieczeństwa informacji i ochrony danych osobowych, audytor wiodący (rola, zadania, uprawnienia), cyberbezpieczeństwo, norma ISO 27002, czarny wywiad, biały wywiad, socjotechnika i jej rodzaje, zarządzanie kryzysowe	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
UMIEJĘTNOŚCI: - potrafi wykorzystywać posiadaną wiedzę – formułować i rozwiązywać złożone i nietypowe problemy z zakresu zarządzania bezpieczeństwem informacji oraz ochrony danych osobowych, a także innowacyjnie wykonywać zadania w nieprzewidywalnych warunkach przez: - właściwy dobór źródeł danych i informacji z nich pochodzących, dokonywanie oceny, krytycznej analizy, syntezy, twórczej interpretacji i prezentacji tych informacji, - dobór oraz stosowanie właściwych metod i narzędzi, w tym zaawansowanych technik informacyjno-komunikacyjnych, - przystosowanie istniejących lub opracowanie nowych metod i narzędzi z zakresu zarządzania - potrafi komunikować się na tematy specjalistyczne z zakresu bezpieczeństwa informacji i ochrony danych osobowych ze zróżnicowanymi - w tym międzynarodowymi - kręgami odbiorców posługując się specjalistyczną terminologią z zakresu nauk o zarządzaniu i jakości - potrafi brać udział w dyskusjach poświęconych zagadnieniom z obszaru bezpieczeństwa informacji i ochrony danych osobowych, zarówno jako uczestnik, jak i prowadzący je - potrafi samodzielnie planować i realizować własne uczenie się przez całe życie i ukierunkowywać innych w tym zakresie wykorzystując zdobytą wiedzę z zakresu zarządzania bezpieczeństwem informacji i ochrony danych osobowych	Definiuje, identyfikuje i rozwiązuje problemy z zakresu bezpieczeństwa informacji i ochrony danych osobowych. Wykorzystuje w praktyce regulacje prawne dotyczące bezpieczeństwa informacji i ochrony danych osobowych, w szczególności akty prawne oraz normy ISO 27001, 27002, 22301, 31000, 27005. Wykorzystuje techniki komunikowania się w kierunku zapewnienia bezpieczeństwa informacji i ochrony danych osobowych, dzięki czemu sprawnie zarządza sytuacjami kryzysowymi z tego obszaru w organizacjach. Poszerza i aktualizuje swoją wiedzę z zakresu bezpieczeństwa informacji i ochrony danych osobowych.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
KOMPETENCJE SPOŁECZNE: - jest gotów do krytycznej oceny posiadanej wiedzy i treści dotyczących bezpieczeństwa informacji i ochrony danych osobowych - jest gotów do uznawania roli i znaczenia wiedzy z zakresu bezpieczeństwa informacji oraz ochrony danych osobowych w rozwiązywaniu problemów poznawczych i praktycznych w zakresie organizacji i zarządzania oraz wyszukiwania informacji i zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu - jest gotów do odpowiedzialnego pełnienia ról menedżera bezpieczeństwa informacji, inspektora danych osobowych oraz audytora systemu zarządzania bezpieczeństwem informacji, zarówno w kontekście lokalnym i globalnym, z uwzględnieniem zmieniających się potrzeb społecznych, w tym: • rozwijania dorobku zawodu, • podtrzymywania etosu zawodu, • przestrzegania i rozwijania zasad etyki zawodowej oraz działania na rzecz przestrzegania tych zasad	Wykorzystując wiedzę i umiejętności z zakresu bezpieczeństwa informacji i ochrony danych osobowych, jest gotowy do dalszego rozwijania się w kierunku ról Inspektora Ochrony Danych Osobowych i/lub Menedżera Bezpieczeństwa Informacji, a także Audytora Wewnętrznego lub Wiodącego. Odpowiedzialnie podchodzi do zdobywania i wykorzystywania uprawnień do pełnienia ww. ról.	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

Świadectwo ukończenia studiów podyplomowych, które otrzymuje absolwent zawiera program kierunku wraz ze zrealizowanymi godzinami i punktami ECTS.

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

Świadectwo ukończenia studiów podyplomowych jest wydawane na podstawie uzyskania zaliczenia każdego przedmiotu zgodnie z Kartą Opisu Przedmiotu oraz po spełnieniu wymagań związanych z ukończeniem studiów podyplomowych, które wskazane zostały w Karcie Opisu Kierunku.

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

Świadectwo ukończenia studiów podyplomowych jest potwierdzeniem uzyskania pozytywnej oceny końcowej, która weryfikowana jest przez 3-osobową komisję egzaminacyjną.

Program

Studia podyplomowe dwusemestralne.

Główny cel usługi został wskazany w celu edukacyjnym

Lp.	Przedmiot	Liczba godzin teoretycznych	Liczba godzin praktycznych	Punkty ECTS
1	Wprowadzenie do bezpieczeństwa informacji i ochrony danych osobowych	4	4	1
2	Nowe kierunki zagrożeń i dostępne zabezpieczenia	8	8	3
3	Ochrona danych osobowych – uwarunkowania prawne w Polsce i na świecie	8	8	1
4	Zadania i odpowiedzialność Inspektora Ochrony Danych Osobowych	4	4	1
5	Zarządzanie bezpieczeństwem informacji w międzynarodowych grupach kapitałowych	4	4	1
6	Praktyczne aspekty tworzenia dokumentacji z zakresu ochrony danych osobowych	6	10	4
7	Zarządzanie ciągłością działania organizacji wg ISO 22301	6	10	2
8	Aspekty prawne związane z incydentami bezpieczeństwa informacji	4	4	1
9	Zarządzanie incydentami bezpieczeństwa informacji	4	4	1
10	Zarządzanie bezpieczeństwem informacji wg normy ISO/IEC 27001	4	4	2
11	Zarządzanie ryzykiem wg norm ISO 31000, ISO 27005 – praktyczne warsztaty	8	8	4
12	Wdrażanie systemu zarządzania bezpieczeństwem informacji zgodnego z ISO/IEC 27001 – praktyczne warsztaty	4	4	2
13	Audytowanie wdrożonego systemu zarządzania wg ISO/IEC 27001 – praktyczne warsztaty	4	12	4
14	Wartość informacji – wywiad gospodarczy a funkcjonowanie przedsiębiorstw	4	4	1
15	Socjotechnika w pozyskiwaniu informacji	4	4	1
16	Efektywna komunikacja w zarządzaniu i sytuacjach kryzysowych	4	4	1
	Razem	**80**	**96**	**30**

Absolwent otrzymuje świadectwo ukończenia studiów podyplomowych, które zawiera program kierunku wraz ze zrealizowanymi godzinami i punktami ECTS.

W czas trwania usługi wykazany w harmonogramie zostały wliczone godziny dydaktyczne wraz z przerwami

Sposób walidacji został ujęty w zakładce: Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji.

Harmonogram

Liczba przedmiotów/zajęć: 12

Przedmiot / temat zajęć	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 12 Wprowadzenie do bezpieczeństwa informacji i ochrony danych osobowych (zajęcia zdalne w czasie rzeczywistym)	16-11-2024	08:55	16:05	07:10
2 z 12 Zadania i odpowiedzialność Inspektora Ochrony Danych Osobowych (zajęcia zdalne w czasie rzeczywistym)	17-11-2024	08:55	16:05	07:10
3 z 12 Ochrona danych osobowych - uwarunkowania prawne w Polsce i na świecie (zajęcia zdalne w czasie rzeczywistym)	30-11-2024	08:55	16:05	07:10
4 z 12 Ochrona danych osobowych - uwarunkowania prawne w Polsce i na świecie (zajęcia zdalne w czasie rzeczywistym)	01-12-2024	08:55	16:05	07:10
5 z 12 Nowe kierunki zagrożeń i dostępne zabezpieczenia (zajęcia zdalne w czasie rzeczywistym)	14-12-2024	08:55	16:05	07:10
6 z 12 Nowe kierunki zagrożeń i dostępne zabezpieczenia (zajęcia zdalne w czasie rzeczywistym)	15-12-2024	08:55	16:05	07:10
7 z 12 Zarządzanie bezpieczeństwem informacji w międzynarodowych grupach kapitałowych (zajęcia zdalne w czasie rzeczywistym)	11-01-2025	08:55	16:05	07:10

Przedmiot / temat zajęć	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
8 z 12 Praktyczne aspekty tworzenia dokumentacji z zakresu ochrony danych osobowych (zajęcia zdalne w czasie rzeczywistym)	12-01-2025	08:55	16:05	07:10
9 z 12 Aspekty prawne związane z incydentami bezpieczeństwa informacji (zajęcia zdalne w czasie rzeczywistym)	25-01-2025	08:55	16:05	07:10
10 z 12 Zarządzanie incydentami bezpieczeństwa informacji (zajęcia zdalne w czasie rzeczywistym)	26-01-2025	08:55	16:05	07:10
11 z 12 Praktyczne aspekty tworzenia dokumentacji z zakresu ochrony danych osobowych (zajęcia zdalne w czasie rzeczywistym)	08-02-2025	08:55	16:05	07:10
12 z 12 Wartość informacji - wywiad gospodarczy a funkcjonowanie przedsiębiorstw (zajęcia zdalne w czasie rzeczywistym)	09-02-2025	08:55	16:05	07:10

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 100,00 PLN
Koszt przypadający na 1 uczestnika netto	4 100,00 PLN

Koszt osobogodziny brutto	23,30 PLN
Koszt osobogodziny netto	23,30 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

mgr Renata Podlewska

Doświadczony manager IT w zakresie wdrażania i audytowania systemów: bezpieczeństwa informacji, opartego na normie ISO 27001, zarządzania usługami opartego na normie ISO 20000, ciągłością działania opartego na normie ISO 22301, zarządzania ryzykiem opartego na normie ISO 31000 oraz wymagań szacowania ryzka IT i cyberbezpieczeństwa wg Dyrektywy NIS2.

Poza tym duże doświadczenie w audytowaniu na zgodność z wymaganiami Krajowych Ram Interoperacyjności, Krajowego Systemu Cyberbezpieczeństwa oraz w zakresie ochrony danych osobowych.

Praktyk z kilkunastoletnim doświadczeniem w zarządzaniu usługami IT, zarządzaniu projektami i audytorka wewnętrzna w korporacji i instytucji publicznej.

Akredytowana trenerka ITIL® SIAM oraz zarządzania Projektami PRINCE2® (Practitioner).

Certyfikowany Inspektor Ochrony Danych.

Inspektor Ochrony Danych w Uniwersytecie Medycznym im. K. Marcinkowskiego w Poznaniu.

Członek zespołu ds. sektora medycznego oraz ds. nowych technologii w Instytucie Prawa Ochrony Danych przy Akademii Ekonomiczno-Humanistycznej i Urzędzie Ochrony Danych Osobowych w Warszawie.

Główny specjalista ds. bezpieczeństwa informacji w Polskim Instytucie Technologicznym.

Audytor Wiodący ISO 27001 i ISO 22301.

Wykładowca akademicki w Uniwersytecie Ekonomicznym w Poznaniu, Uniwersytecie Ekonomicznym w Katowicach, Uniwersytecie Medycznym w Poznaniu.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały dydaktyczne (pliki dokumentów przygotowanych w dowolnych formach) przekazywane są uczestnikom w formie elektronicznej.

Warunki uczestnictwa

Warunkiem przyjęcia na studia jest ukończenie studiów I, II stopnia lub jednolitych studiów magisterskich.

Informacje dodatkowe

1. **CENA STUDIÓW MOŻE ULEC ZMIANIE,** ze względu na przewidziane Zarządzeniem Rektora zniżki w czesnym lub dodatkową opłatę za rozłożenie płatności na raty: https://bap.ue.katowice.pl/423-lista/d/4004/5/ (z późn. zm.)
2. Kadra naukowo-dydaktyczna obejmuje więcej osób prowadzących zajęcia niż jest zamieszczonych w karcie usługi.
3. Oprócz rejestracji w BUR należy zarejestrować się w systemie internetowej rekrutacji IRK2 Uczelni.
4. Termin rejestracji w systemie IRK2 Uczelni upływa dnia 06.11.2024r.
5. Godziny rozpoczęcia zajęć oraz ich zakończenia zostały podane w harmonogramie jako godziny dyspozycyjności uczestnika (wraz z przerwami). Liczba godzin usługi jest podana w godzinach dydaktycznych.
6. Szczegółowy harmonogram wraz z salami oraz wszelkie informacje dostępne na stronie (https://www.ue.katowice.pl/studia-podyplomowe/obsluga-sluchaczy/harmonogramy-zjazdow.html)
7. Więcej informacji: https://www.ue.katowice.pl/studia-podyplomowe.html
8. Brak możliwości rozliczania się za pośrednictwem Bonów Rozwojowych.

Warunki techniczne

Do wszystkich zajęć niezbędny jest komputer lub inne urządzenie ze stałym łączem internetowym. Zajęcia prowadzone są na platformie e-learningowa G Suite - Google Classroom, Google Meet. Logowanie możliwe jest tylko z adresów w domenie edu.uekat.pl (uczestnicy). Każdy uczestnik studiów podyplomowych otrzymuje indywidualne konto w usłudze Google Apps. Sygnały wychodzące od uczestnika we wszystkich sytuacjach muszą spełniać wymagania przepustowości 3,2 mbps . Sygnały przychodzące zależą od liczby uczestników: 4,0 Mb/s przy 10 uczestnikach.

Kontakt

Magdalena Gogolińska

E-mail magdalena.gogolinska@ue.katowice.pl
Telefon (+48) 322 577 769