



Studia podyplomowe - Zarządzanie i ochrona informacji niejawnych i danych osobowych

Numer usługi 2025/12/05/180566/3193605

3 800,00 PLN brutto
3 800,00 PLN netto
20,00 PLN brutto/h
20,00 PLN netto/h

PODKARPACKA
SZKOŁA WYŻSZA
IM.BŁ.KS.WŁADYSŁ
AWA FINDYSZA W
JAŚLE

Brak ocen dla tego dostawcy

📍 zdalna w czasie rzeczywistym
📖 Studia podyplomowe
🕒 190 h
📅 26.03.2026 do 26.02.2027

Informacje podstawowe

Kategoria

Prawo i administracja / Ochrona informacji niejawnych

Grupa docelowa usługi

Studia skierowane są do osób odpowiedzialnych za bezpieczeństwo informacji w sektorze publicznym, prywatnym oraz w służbach mundurowych. Ofertę dedykujemy w szczególności:

- **Funkcjonariuszom i żołnierzom:** przedstawicielom Policji, Straży Granicznej, Straży Pożarnej oraz żołnierzom Wojska Polskiego (ze szczególnym uwzględnieniem Wojsk Obrony Terytorialnej) i pracownikom cywilnym wojska.
- **Administracji i Służbie Zdrowia:** pracownikom urzędów, agencji rządowych i samorządowych oraz ratownikom medycznym i koordynatorom służb ratunkowych.
- **Sektorowi Biznesowemu:** kadry bankowości, ubezpieczeń oraz firm z sektorów infrastruktury krytycznej (energetyka, transport, telekomunikacja).
- **Specjalistom ds. bezpieczeństwa:** Pełnomocnikom ds. ochrony informacji niejawnych, Inspektorom Ochrony Danych (IOD) oraz osobom zarządzającym pionami ochrony.

Minimalna liczba uczestników

15

Maksymalna liczba uczestników

35

Data zakończenia rekrutacji

23-03-2026

Forma prowadzenia usługi

zdalna w czasie rzeczywistym

Liczba godzin usługi

190

Cel

Cel edukacyjny

Celem jest przygotowanie do pełnienia funkcji Pełnomocnika ds. Ochrony Informacji Niejawnych, Inspektora Ochrony Danych oraz kierownika kancelarii tajnej. Uczestnik zdobędzie wiedzę niezbędną do organizowania systemu ochrony informacji w administracji, służbach mundurowych i biznesie. Program uczy tworzenia polityk bezpieczeństwa, zarządzania ryzykiem oraz procedur ochrony fizycznej i osobowej. Absolwent będzie gotowy do samodzielnej ochrony danych wrażliwych przed nieuprawnionym ujawnieniem.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozróżnia systemy prawne ochrony danych (UE vs krajowe). Zna hierarchię aktów prawnych (Konstytucja, Ustawy). Interpretuje przepisy Ustawy o ochronie informacji niejawnych.	Wymienia klauzule tajności (zastrzeżone, poufne, tajne, ściśle tajne). Wskazuje różnice między tajemnicą zawodową a państwową.	Test teoretyczny
Definiuje kluczowe zasady RODO (rozliczalność, minimalizacja). Rozumie prawa osób, których dane dotyczą. Stosuje przepisy RODO w praktyce organizacji.	Wymienia przesłanki legalności przetwarzania danych. Wyjaśnia zasadę privacy by design. Rozwiązuje kasus dotyczący obowiązku informacyjnego.	Test teoretyczny
Projektuje procesy przetwarzania danych w organizacji. Zarządza cyklem życia danych (od pozyskania do usunięcia). Nadzoruje przepływ danych między działami.	Mapuje procesy przetwarzania danych w firmie. Identyfikuje zbiory danych wymagające szczególnej ochrony.	Analiza dowodów i deklaracji
Sporządza wymaganą dokumentację (RCP, klauzule, upoważnienia). Prowadzi Rejestr Czynności Przetwarzania. Aktualizuje polityki bezpieczeństwa zgodnie ze zmianami.	Przygotowuje projekt klauzuli informacyjnej. Wypełnia przykładowy Rejestr Czynności Przetwarzania (RCP). Tworzy wzór upoważnienia do przetwarzania danych.	Analiza dowodów i deklaracji
Zna procedury skargowe do Prezesa UODO. Definiuje środki ochrony cywilnej i sądowej. Doradza w kwestii ścieżki prawnej w przypadku naruszeń.	Opisuje procedurę kontroli UODO. Wymienia roszczenia przysługujące osobie, której prawa naruszono	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Identyfikuje ryzyka prawne i finansowe dla organizacji. Zna taryfikator kar administracyjnych RODO. Rozróżnia odpowiedzialność karną, cywilną i dyscyplinarną.	Analizuje przypadek naruszenia i szacuje potencjalną karę. Wymienia przesłanki łagodzące wymiar kary administracyjnej.	Analiza dowodów i deklaracji
Przeprowadza analizę ryzyka dla zasobów informacyjnych. Dobiera środki techniczne i organizacyjne (zabezpieczenia fizyczne, IT). Wdraża Normy ISO/IEC 27001 w zakresie bezpieczeństwa.	Dokonuje szacowania ryzyka prostą metodą (np. macierz ryzyka). Proponuje zabezpieczenia dla serwerowni i archiwum.	Obserwacja w warunkach symulowanych
Planuje i przeprowadza audyt zgodności z RODO/KRI. Weryfikuje skuteczność zabezpieczeń. Raportuje niezgodności i rekomenduje działania naprawcze.	Opracowuje listę kontrolną (checklistę) do audytu. Sporządza fragment raportu z audytu wskazujący uchybienia.	Analiza dowodów i deklaracji
Definiuje rolę, zadania i pozycję IOD w strukturze. Rozumie zasady niezależności Inspektora. Wspiera administratora w realizacji obowiązków.	Wymienia zadania ustawowe IOD. Symuluje rozmowę doradczą z zarządem firmy. Wskazuje sytuacje konfliktu interesów IOD.	Wywiad swobodny
Konstruuje umowy powierzenia przetwarzania danych. Weryfikuje podmioty przetwarzające (procesorów). Nadzoruje transfery danych do państw trzecich.	Analizuje draft umowy powierzenia pod kątem wymogów art. 28 RODO. Wskazuje mechanizmy legalizujące transfer danych poza EOG.	Analiza dowodów i deklaracji
Analizuje studia przypadków wycieków danych (Data Breach). Identyfikuje najczęstsze błędy ludzkie i systemowe. Wdraża procedury zgłaszania naruszeń.	Omawia przyczyny realnego wycieku danych (case study). Wypełnia formularz zgłoszenia naruszenia do UODO. Proponuje działania zapobiegawcze na przyszłość.	Prezentacja

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

TAK

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

TAK

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

TAK

Program

Podstawy prawne dotyczące danych osobowych i informacji niejawnych,
RODO,
Zarządzanie danymi osobowymi,
Dokumentacja w zakresie danych osobowych,
Środki ochrony prawnej,
odpowiedzialność i sankcje,
Zarządzanie bezpieczeństwem informacji,
Audytowanie procesów bezpieczeństwa,
Inspektor Ochrony Danych Osobowych,
Przetwarzanie danych
Uchybienia i błędy w praktyce urzędów i instytucji w zakresie ochrony informacji niejawnych i danych.
Czas trwania: 2 semestry. Umożliwiają uzyskanie 30 punktów ECTS.
Łączna ilość godzin: 190 godzin dydaktycznych (godzina dydaktyczna trwa 45 minut). Zajęcia na studiach prowadzone są w formie ćwiczeń oraz wykładów.
Przerwy w zajęciach nie wliczają się do godzin dydaktycznych. Przerwę ustala i komunikuje wykładowca.
Walidacja: słuchacz studiów podyplomowych uzyskuje zaliczenie lub ocenę po zakończeniu każdego przedmiotu. Po zakończeniu zajęć dydaktycznych, uzyskaniu zaliczeń z wszystkich przedmiotów dopuszczany jest do egzaminu końcowego. Po pozytywnym zdaniu egzaminu końcowego uzyskuje świadectwo ukończenia studiów podyplomowych.

Harmonogram

Liczba przedmiotów/zajęć: 0

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Cennik

Rodzaj ceny	Cena
-------------	------

Koszt przypadający na 1 uczestnika brutto	3 800,00 PLN
Koszt przypadający na 1 uczestnika netto	3 800,00 PLN
Koszt osobogodziny brutto	20,00 PLN
Koszt osobogodziny netto	20,00 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy student otrzyma:

- Konto pocztowe o pojemności 50Gb.
- Chmurę OneDrive o pojemności 1Tb w której może przetrzymywać dowolne pliki np. materiały do zajęć czy różne projekty.
- Dostęp do aplikacji Word, Excel, Power Point w przeglądarce - dzięki zastosowaniu Chmury OneDrive studenci mogą wspólnie wykonywać prace grupową.

Warunki uczestnictwa

Wykształcenie wyższe (co najmniej licencjat/inżynier)

– wymagane do podjęcia studiów podyplomowych.

Złożenie kompletu wymaganych dokumentów,

- Formularz rekrutacyjny (dostępny w punkcie rekrutacyjnym - czyli dziekanacie PSW lub Internecie na stronie www.psw.jaslo.pl),
- odpis dyplomu ukończenia studiów wyższych lub oryginalny dyplom. W przypadku ukończenia uczelni wyższej za granicą kandydat składa oryginał dyplomu oraz jego tłumaczenie na język polski potwierdzone przez upoważnione instytucje, a także dokument potwierdzający nostryfikację dyplomu lub zaświadczenie o zwolnieniu z postępowania nostryfikacyjnego,
- dowód wpłaty czesnego i wpisowego

Opłata za udział w studiach

– zgodnie z cennikiem uczelni (z możliwością dofinansowania z BUR, jeśli uczestnik spełnia kryteria).

Aktywne uczestnictwo w zajęciach i zaliczenie końcowych form sprawdzających

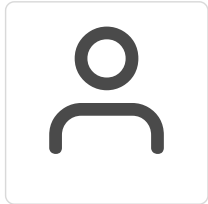
Informacje dodatkowe

Program studiów charakteryzuje się unikalnym podziałem na dwa moduły: semestr pierwszy poświęcony jest **Zarządzaniu i ochronie informacji niejawnych**, a drugi **Zarządzaniu danymi osobowymi i bezpieczeństwu informacji**. Taka struktura porządkuje materiał i pozwala na dogłębne poznanie najnowszych, efektywnych form ochrony informacji, bazujących na standardach polskich i zagranicznych.

Warunki techniczne

- Uczestnicy muszą posiadać **stabilne łącze internetowe** o minimalnej prędkości 10 Mbps.
- Wymagany jest **komputer, laptop, tablet lub smartfon** z dostępem do kamery i mikrofonu.
- Zalecane jest korzystanie z najnowszej wersji przeglądarki internetowej (np. Chrome, Firefox, Edge).
- Zajęcia prowadzone są na platformie Teams
- Platforma e-learningowa zapewnia **dostęp do uczestnictwa w zajęciach na żywo** oraz konsultacji z wykładowcami.
- Wymagane jest przestrzeganie zasad etykiety online oraz aktywny udział w zajęciach.

Kontakt



Lucyna Mamroł

E-mail lmamrol@psw.jaslo.pl

Telefon (+48) 533 801 602