WYŻSZA SZKOŁA BIZNESU
W DĄBROWIE GÓRNICZEJ
CENTRUM STUDIÓW PODYPLOMOWYCH I REKRUTACJI
BIELSKO-BIAŁA, BYTOM, CIESZYN, CZĘSTOCHOWA, DĄBROWA GÓRNICZA, KRAKÓW, OLKUSZ, ŻYWIEC

Kontakt:
Centrum Studiów Podyplomowych i Rekrutacji
tel.: 32 262 28 05
e-mail.: podyplomowe@wsb.edu.pl

OCHRONA DANYCH OSOBOWYCH W ADMINISTRACJI I BIZNESIE

INSPEKTOR OCHRONY DANYCH

Czas trwania: 2 semestry/160 godz.

Liczba ECTS: 60

Czesne: 4500 zł
6 rat: (wpisowe 300 zł, 4x800 zł, 1x700 zł, 1x300 zł)

CEL:

Celem studiów jest podnoszenie kwalifikacji pracowników administracji publicznej i innych podmiotów organizacyjnych mających w swej działalności do czynienia z danymi osobowymi, w szczególności administratorów bezpieczeństwa informacji oraz wykształcenie specjalistów zajmujących się tworzeniem systemu skutecznej ochrony strategicznych informacji przedsiębiorstw lub instytucji oraz przygotowanie specjalistów do pełnienia funkcji Administratora Bezpieczeństwa Informacji, Administratora Danych Osobowych.

UCZESTNICY STUDIÓW:

Studia skierowane są głównie do osób zajmujących się szeroko rozumianą problematyką ochrony informacji, w tym biznesowych i danych osobowych we wszystkich sektorach gospodarki (pracownicy przedsiębiorstw i firm, administracji państwowej i samorządowej), czyli do osób, które kierują lub przygotowują się do pracy w pionach ochrony danych osobowych i informacji niejawnych lub odpowiadają za politykę bezpieczeństwa w swoich jednostkach organizacyjnych.

SPOSÓB ZALICZENIA STUDIÓW:

- po I semestrze nauki – test zaliczeniowy,
- po II semestrze nauki – test zaliczeniowy.

W PROGRAMIE:

1. Zasady ochrony danych osobowych w działalności instytucji publicznych i sektora prywatnego
2. Podstawy prawne ochrony informacji niejawnych
3. Praktyczne aspekty tworzenia dokumentacji z zakresu ochrony danych osobowych oraz realizacji zadań administratora bezpieczeństwa informacji
4. Ochrona informacji niejawnych: bezpieczeństwo osobowe, przemysłowe, teleinformatyczne
5. Pomiar bezpieczeństwa
6. Zasady prowadzenie audytów systemów zarządzania
7. Zarządzanie incydentami bezpieczeństwa
8. Zarządzanie ciągłością działania w tym administracji publicznej
9. Zarządzanie ryzykiem w bezpieczeństwie informacji
10. Bezpieczeństwo informacji biznesowych. Teoretyczne i praktyczne aspekty ustanawiania i wdrażania tajemnicy przedsiębiorstwa
11. Systemy zarządzania jakością i bezpieczeństwem informacji
12. Praktyka prowadzenia audytów
13. Funkcjonowanie pionu ochrony informacji niejawnych w praktyce. Prowadzenie kancelarii tajnej i niejawnej
14. Nowoczesne techniki technologii i ochrony informacji
15. Szacowanie i zarządzanie ryzykiem w ochronie informacji niejawnych
16. Pracownia problemowa
17. Informacja publiczna
18. Kontrole GIODO – zakres, treść, obowiązki kontrolowanych
19. Wykład monograficzny
20. Konsultacje
21. Analiza ryzyka i ocena zagrożeń w świetle przepisów ogólnego rozporządzenia o ochronie danych osobowych
22. Praktyczne aspekty tworzenia klauzul zgód i klauzul informacyjnych w kontekście realizacji uprawnień podmiotów danych