Uniwersytet Wrocławski

WYDZIAŁ PRAWA, ADMINISTRACJI I EKONOMII

SEKCJA OBSŁUGI STUDIÓW DOKTORANCKICH I INNYCH FORM KSZTAŁCENIA
ul. Uniwersytecka 22/26
50-145 Wrocław

tel. +48 71 375 23 71

podyplomowe.wpae@uwr.edu.pl | www.podyplomowe.prawo.uni.wroc.pl

Wrocław, dnia 13 czerwca 2018 r.

Uniwersytet Wrocławski
Wydział Prawa, Administracji i Ekonomii
ogłasza zapisy na kurs
Audytor wewnętrzny SZBI zgodnego z ISO 27001 jako narzędzie realizacji wymagań RODO

Termin kursu: 16-17 czerwca 2018 r.
Koszt: 1100 PLN (tysiąc sto złotych), płatne zgodnie z postanowieniami umowy o świadczeniu usług edukacyjnych; na wskazany w ofercie rachunek bankowy; brak opłaty rekrutacyjnej.
Specjalna zniżka dla Absolwentów Studiów Podyplomowych Ochrony Danych Osobowych Wydziału Prawa, Administracji i Ekonomii UWr w wysokości 20%.
Warunki przyjęcia: wypełnienie formularza zgłoszeniowego oraz umowy i uiszczenie opłaty w wysokości 1100 PLN, do dnia 13 czerwca 2018 r. na rachunek bankowy Uczelni /Wydziału: **68 1090 2503 0000 0001 0246 5849**

Szkolący:
Prof. dr hab. Mariusz Jabłoński, r.pr – pracownik UWr, praktyk
Dr Krzysztof Wygoda – pracownik UWr, praktyk
Mgr inż. Tomasz Radziszewski – praktyk

W ramach szkolenia uczestnicy otrzymują materiały dydaktyczne.

HARMONOGRAM ZAJĘĆ

Dzień pierwszy ***/ sala 2.05 D (budynek D Wydziału Prawa, Administracji i Ekonomii, ul. Uniwersytecka 7-10)***

I blok szkoleniowy: 09:00 – 12:00 (przerwy kawowe wg potrzeb uczestników kursu)
1. Siatka pojęć podstawowych związanych z ochroną informacji;
2. Burzliwe otoczenie organizacji, wymagania prawne związane z ochroną informacji;

a) Jawność a system ochrony informacji (prawa jednostki, obowiązki administratora systemu zarządzania bezpieczeństwem informacji (SZBI), ramy bezpieczeństwa na gruncie przepisów o informatyzacji),
b) Udostępnianie aktywów informacyjnych na gruncie przepisów szczególnych tworzących wyjątki w zasadzie zachowania poufności, dostępności i integralności procesów przetwarzania aktywów informacyjnych (obowiązki administratora SZBI)

3. Potrzeby organizacji w zakresie bezpieczeństwa;
4. Definiowanie zakresu systemu, analiza aktywów informacyjnych;
5. Polityka bezpieczeństwa jako przejaw przywództwa;
6. Cele związane z ochroną informacji, ryzyka i szanse;

II blok szkoleniowy: 12:00 – 14:00 (przerwy wg potrzeb uczestników kursu)
1. Struktura funkcjonalna, kompetencje i uprawnienia (rola IOD i administratora danych osobowych, zespół ds. oceny ryzyka związanego z ochroną informacji – jego rola w ramach oceny skutków dla ochrony danych osobowych);
2. Bezpieczeństwo osobowe;

3. Bezpieczeństwo fizyczne.

Przerwa na lunch 14:00 – 14:30

III blok szkoleniowy: 14:30 – 16:00 (przerwy wg potrzeb uczestników szkolenia)

1. Siatka pojęć podstawowych związanych z zarządzaniem ryzykiem;
2. Szacowanie ryzyka, postępowanie z ryzykiem – przygotowanie do ćwiczenia.
3. Podstawowa siatka pojęć związanych z zarządzaniem ciągłością działania;
4. Analiza krytycznych i kluczowych procesów biznesowych (BIA);

Dzień drugi ***/ sala 2.05 D (budynek D Wydziału Prawa, Administracji i Ekonomii, ul. Uniwersytecka 7-10)***

I blok szkoleniowy: 09:00 – 12:00 (przerwy wg potrzeb uczestników kursu)

1. Systemowe podejście do analizy i szacowania ryzyka;
2. Analiza zagrożeń i podatności związanych z aktywami – ćwiczenie;
3. Metodyka szacowania ryzyka, estymacja ryzyk – ćwiczenie;
4. Dokumentowanie procesu szacowania ryzyka (oceny skutków dla ochrony danych osobowych) oraz postępowania z ryzykiem;
5. Dokumentowanie Polityki Zarządzania Ciągłością Działania (Plan zarządzania ciągłością działania, definiowanie scenariuszy awaryjnych);

II blok szkoleniowy: 12:00 – 14:00 (przerwy wg potrzeb uczestników kursu)

1. Planowanie audytów, techniki audytowania;
2. Posługiwanie się wzorcowym wykazem celów zabezpieczania i zabezpieczeń cz. 1;

Przerwa na lunch 14:00 – 14:30

III blok szkoleniowy: 14:30 – 15:30

1. Posługiwanie się wzorcowym wykazem celów zabezpieczania i zabezpieczeń cz. 2;

15:30-16:00 Egzamin pisemny