Możliwość dofinansowania

edpo.pl Michał Cupiał

★★★★★

Razem wzmacniamy bezpieczeństwo: skuteczne zarządzanie ryzykiem w kontekście bezpieczeństwa informacji. Praktyczne szkolenie.

Numer usługi 2024/11/20/160750/2422080

Olsztyn / stacjonarna
Usługa szkoleniowa
10 h
14.12.2024 do 14.12.2024

2 400,00 PLN brutto
2 400,00 PLN netto
240,00 PLN brutto/h
240,00 PLN netto/h

Informacje podstawowe

Kategoria	Prawo i administracja / Prawo Unii Europejskiej
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Usługa kierowana jest do: • osób prowadzących działalność gospodarczą, • kierownictwa i zarządu przedsiębiorstw z sektora MMŚP, podejmujących decyzje strategiczne dotyczące bezpieczeństwa informacji, • liderów lub przyszłych liderów zespołów odpowiedzialnych za operacyjne zarządzanie IT i/lub ochronę danych osobowych, • osób chcących zdobywać nowe kompetencje w zakresie zarządzania ryzykiem.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	5
Data zakończenia rekrutacji	11-12-2024
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	10
Podstawa uzyskania wpisu do BUR	Certyfikat VCC Akademia Edukacyjna

Cel

Cel edukacyjny

Usługa przygotowuje uczestników do zarządzania ryzykiem w przedsiębiorstwie, skoncentrowanego na bezpieczeństwie informacji i ochronie danych osobowych, poprzez zdobycie umiejętności i kompetencji pozwalających na skutecznie identyfikowanie i ocenianie ryzyka. Szkolenie zapewni uczestnikom wiedzę dotyczącą tworzenia i wdrażania efektywnych strategii zarządzania ryzykiem, zgodne z przepisami prawnymi i najlepszymi praktykami branżowymi.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik uzyskuje umiejętność identyfikowania zagrożeń związanych z bezpieczeństwem informacji i ochroną danych osobowych.	identyfikuje zagrożenia związane z bezpieczeństwem informacji,	Test teoretyczny
	klasyfikuje zagrożenia na podstawie ich potencjalnego wpływu na organizację	Test teoretyczny
Uczestnik uzyskuje umiejętność oceny ryzyka i jego wpływu na przedsiębiorstwo	identyfikuje ryzyko	Test teoretyczny
	identyfikuje prawdopodobieństwo wystąpienia incydentów oraz ich potencjalne skutki	Test teoretyczny
Uczestnik uzyskuje umiejętność tworzenia strategii zarządzania ryzykiem	projektuje strategie zarządzania ryzykiem, uwzględniając specyfikę organizacji i obowiązujące przepisy prawne	Test teoretyczny
Uczestnik uzyskuje umiejętność wdrożenia technicznych i organizacyjnych środków bezpieczeństwa	projektuje strategie wdrożenia konkretnych środków bezpieczeństwa	Test teoretyczny
Uczestnik uzyskuje umiejętność reagowania na incydenty bezpieczeństwa	identyfikuje incydenty, które mogą skutkować naruszeniem bezpieczeństwa informacji	Test teoretyczny
Uczestnik uzyskuje umiejętność kształtowania kultury organizacyjnej sprzyjającej bezpieczeństwu informacji i ochronie danych, poprzez organizacje szkoleń i kampanii edukacyjnych dla pracowników	definiuje działania promujące kulturę bezpieczeństwa informacji	Test teoretyczny
Uczestnik uzyskuje umiejętność raportowania zarządzanym ryzykiem oraz przedstawiania rekomendacji, np.: zarządowi i interesariuszom.	przygotowuje raporty z zarządzanego ryzyka	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

Tak, dokument potwierdzający uzyskanie kompetencji (certyfikat) zawiera opis efektów uczenia się w postaci suplementu.

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

Tak. Dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji.

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

Tak. Dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji.

Program

Usługa **„Razem wzmacniamy bezpieczeństwo: skuteczne zarządzanie ryzykiem w kontekście bezpieczeństwa informacji. Praktyczne szkolenie."** przygotowuje uczestników do zarządzania ryzykiem w przedsiębiorstwie, skoncentrowanego na bezpieczeństwie informacji i ochronie danych osobowych, poprzez zdobycie umiejętności i kompetencji pozwalających na skutecznie identyfikowanie i ocenianie ryzyka.

Szkolenie zapewni uczestnikom wiedzę dotyczącą tworzenia i wdrażania efektywnych strategii zarządzania ryzykiem, zgodne z przepisami prawnymi i najlepszymi praktykami branżowymi.

Techniki aktywne podczas zajęć: prezentacja przygotowana przez trenera oraz aktywna dyskusja (z możliwością omówienia dokumentacji wdrożonej w przedsiębiorstwie).

Program ramowy obejmuje:

1. Wprowadzenie do zarządzania ryzykiem w kontekście bezpieczeństwa informacji (Zrozumienie podstawowych pojęć związanych z bezpieczeństwem informacji i ochroną danych osobowych. Przegląd regulacji prawnych. Rodzaje zagrożeń: cyberzagrożenia, zagrożenia fizyczne, ryzyka operacyjne)
2. Proces zarządzania ryzykiem w bezpieczeństwie informacji (Etapy procesu zarządzania ryzykiem: identyfikacja, ocena, reakcja, monitorowanie. Techniki identyfikacji ryzyka: analiza zagrożeń i podatności, ocena ryzyka. Narzędzie oceny ryzyka: macierz ryzyka, analiza wpływu, analiza prawdopodobieństwa)
3. Przerwa (11:00 – 11:15)
4. Ocena i analiza ryzyka w ochronie danych osobowych (Ocena prawdopodobieństwa i wpływu naruszeń danych osobowych. Analiza ilościowa i jakościowa ryzyka w ochronie danych. Techniki oceny ryzyka: DPIA, analiza skutków naruszeń)
5. Strategie zarządzania ryzykiem (Unikanie ryzyka, redukcja ryzyka, akceptacja ryzyka, transfer ryzyka. Narzędzia i techniki zarządzania ryzykiem: wdrażanie środków technicznych i organizacyjnych, polityk bezpieczeństwa, szyfrowania, regularnych audytów)
6. Implementacja zarządzania ryzykiem w przedsiębiorstwie (Struktura organizacyjna a zarządzanie ryzykiem. Rola zarządu, koordynatora ds. ochrony danych osobowych lub Inspektora Ochrony Danych i pracowników w procesie zarządzania ryzykiem)
7. Monitorowanie i raportowanie ryzyka (Metody monitorowania ryzyka: audyty, przeglądy. Techniki raportowania ryzyka: raporty okresowe. Komunikacja ryzyka w firmie i do organów nadzoru)
8. Przerwa (14:15 – 14:30)
9. Podsumowanie głównych tematów poruszonych podczas szkolenia. Sesja pytań.
10. Walidacja – test teoretyczny

Czas trwania usługi:

Szkolenie w postaci wykładu odbędzie się w ciągu jednego dnia szkoleniowego i składa się z 10 godzin dydaktycznych (1 godzina dydaktyczna = 45 minut zegarowych) przeprowadzonych w czasie rzeczywistym w formie stacjonarnej w opisanej lokalizacji.

Do czasu usługi wliczony jest proces walidacji (trwający 45 minut), który odbędzie się w postaci testu teoretycznego (jednokrotnego lub wielokrotnego wyboru w zależności od rodzaju pytania) sprawdzających zdobytą wiedzę i umiejętności.

Harmonogram szkolenia przewiduje 2 przerwy trwające po 15 minut (przerwy nie są wliczane do czasu trwania usługi).

Uczestnicy podczas kursu nie będą podzieleni na grupy.

Kurs adresowany jest dla uczestników znajdujących się w opisanej grupie docelowej, tj. osób prowadzących działalność gospodarczą, kierownictwa i zarządu przedsiębiorstw z sektora MMŚP, podejmujących decyzje strategiczne dotyczące bezpieczeństwa informacji, jak również do liderów zespołów odpowiedzialnych za operacyjne zarządzanie IT i/lub ochronę danych osobowych.

Walidacja:

Proces walidacji odbędzie się po zakończeniu procesu kształcenia, w tym samym dniu usługi.

Walidacja odbędzie się w postaci testu teoretycznego (jednokrotnego lub wielokrotnego wyboru w zależności od rodzaju pytania) sprawdzającego zdobytą wiedzę i umiejętności.

Walidacja zostanie przeprowadzona w formie stacjonarnej.

Proces walidacji będzie oddzielony od procesu kształcenia się w następujący sposób: test teoretyczny zostanie przeprowadzony przez doświadczonego trenera.

Osoba walidująca waliduje usługę, a następnie potwierdza osiągnięcie efektów kształcenia swoim podpisem na certyfikacie.

Harmonogram

Liczba przedmiotów/zajęć: 8

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 8 Wprowadzenie do zarządzania ryzykiem w kontekście bezpieczeństwa informacji	Maciej Grabowski	14-12-2024	08:00	09:30	01:30
2 z 8 Proces zarządzania ryzykiem w bezpieczeństwie informacji	Maciej Grabowski	14-12-2024	09:30	11:00	01:30
3 z 8 Ocena i analiza ryzyka w ochronie danych osobowych	Maciej Grabowski	14-12-2024	11:15	12:00	00:45

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
4 z 8 Strategie zarządzania ryzykiem	Maciej Grabowski	14-12-2024	12:00	12:45	00:45
5 z 8 Implementacja zarządzania ryzykiem w przedsiębiorstwie	Maciej Grabowski	14-12-2024	12:45	13:30	00:45
6 z 8 Monitorowanie i raportowanie ryzyka	Maciej Grabowski	14-12-2024	13:30	14:15	00:45
7 z 8 Podsumowanie głównych tematów poruszonych podczas szkolenia. Sesja pytań	Maciej Grabowski	14-12-2024	14:30	15:15	00:45
8 z 8 Walidacja - test teoretyczny	-	14-12-2024	15:15	16:00	00:45

Cennik

Cennik

Rodzaj ceny	Cena
Koszt usługi brutto	2 400,00 PLN
Koszt usługi netto	2 400,00 PLN
Koszt godziny brutto	240,00 PLN
Koszt godziny netto	240,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Maciej Grabowski

Obszar specjalizacji: ISO 27001, bezpieczeństwo informacji, cyberbezpieczeństwo, ochrona danych osobowych, zarządzanie ryzykiem. Ukończył studia podyplomowe: Audyt i kontrola wewnętrzna na UWM w Olsztynie (2018-2019), Zarządzanie Bezpieczeństwem Informacji na WSAiB w Gdyni (2017-2018). Odbyte kursy i szkolenia: Audytor Wiodący ISO/IEC 27001, Menadżer Bezpieczeństwa Informacji – TUV-NORD (2023), Praktyczne zastosowanie standardów ISO/IEC 27017 i ISO/IEC 27018 – TriSec Consulting.
Doświadczenie zawodowe: doradca w podmiotach z wielu branż w zakresie wdrażania, utrzymywania i monitorowania systemów zarządzania bezpieczeństwem informacji (ISMS) oraz spełnienia przepisów ogólnego rozporządzenia o ochronie danych (RODO). Inspektor Ochrony Danych w jednej z największych polskich firm zajmujących się branżą IT i systemów państwowych. Wspiera podmioty z różnych sektorów w efektywnym zarządzaniu bezpieczeństwem informacji i zarządzaniu ryzykiem i zgodności z RODO. Trener, specjalizujący się w szkoleniach z zakresu bezpieczeństwa informacji, cyberhigieny oraz RODO. W latach 2023-2024 przeprowadził kilkadziesiąt godzin szkoleń z zakresu: bezpieczeństwa informacji oraz ochrony danych osobowych. Pasjonat bezpieczeństwa informacji i cyberbezpieczeństwa. Niezależny audytor RODO i ISO/IEC 27001.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Na materiały dla uczestników składać się będzie prezentacja obejmująca prezentowaną w trakcie szkolenia tematykę oraz ewentualne wytworzone w trakcie trwania szkolenia materiały, które zostaną przesłane uczestnikom w formie elektronicznej po zakończeniu usługi.

Każdy z uczestników po pozytywnej ocenie procesu walidacji końcowej (testu teoretycznego) otrzyma również certyfikat poświadczający ukończenie szkolenia wraz z suplementem zawierającym opis efektów uczenia się.

Warunki uczestnictwa

Uczestnicy warsztatów muszą znajdować się w opisanej grupie docelowej.

Warunkiem uczestnictwa jest zarejestrowanie i założenie konta w Bazie Usług Rozwojowych, zapisanie się na szkolenie za pośrednictwem Bazy i przypisanego ID wsparcia oraz spełnienie wszystkich warunków uczestnictwa w projekcie określonych przez Operatora.

Usługa odbywa się w godzinach dydaktycznych, czyli 1 godzina szkolenia równa się 45 minut zegarowych.

Adres

ul. Jagiellońska 59/212
10-283 Olsztyn
woj. warmińsko-mazurskie

Szkolenie odbędzie się w siedzibie Europejskiej Akademii Medycznych i Społecznych Nauk Stosowanych.
Lokal nr: 212 (II piętro)

Udogodnienia w miejscu realizacji usługi

- Wi-fi

Kontakt

Anna Smolińska

E-mail anna.smolinska@edpo.pl

Telefon (+48) 881 536 777