Możliwość dofinansowania

Kompetencje cyfrowe: Bezpieczeństwo cyfrowe oraz ochrona danych osobowych w przedsiębiorstwie.

Numer usługi 2024/05/14/7675/2148413

5 350,50 PLN brutto
4 350,00 PLN netto
222,94 PLN brutto/h
181,25 PLN netto/h

Zakłady Badań i Atestacji "ZETOM" im. prof. F. Stauba w Katowicach Spółka z ograniczoną odpowiedzialnością

★★★★★

Katowice / stacjonarna
Usługa szkoleniowa
24 h
09.09.2024 do 11.09.2024

Informacje podstawowe

Kategoria	Biznes / Zarządzanie przedsiębiorstwem
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	właściciele, współwłaściciele, kadra menadżerska, osoby przewidziane do awansu na kierownicze stanowisko, osoby zarządzające transformacją cyfrową w przedsiębiorstwie, pracownicy każdego przedsiębiorstwa, którzy mają kontakt z danymi osobowymi oraz informacjami poufnymi, wszystkie osoby zainteresowane tematem, osoby zajmujące się obsługą systemów informatycznych, administrowaniem baz danych, obsługą klientów oraz pracowników HR
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	25
Data zakończenia rekrutacji	08-09-2024
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	24
Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Uczestnicy podniosą świadomość w zakresie zagrożeń związanych z korzystaniem z systemów informatycznych oraz przetwarzaniem danych osobowych. Zwiększą kompetencje w zakresie przestrzegania obowiązujących przepisów dotyczących ochrony danych osobowych (RODO). Zwiększą gotowość na ewentualne incydenty związane z naruszeniem bezpieczeństwa danych oraz przygotują się do skutecznej reakcji w przypadku wystąpienia zagrożeń.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik zwiększa świadomość na temat poziomu bezpieczeństwa organizacji i zminimalizowania ryzyka związanego z utratą, ujawnieniem lub uszkodzeniem informacji poufnej	zmniejszenie liczby incydentów związanych z utratą, ujawnieniem lub uszkodzeniem informacji poufnej, a także poprawa wyników testów bezpieczeństwa oraz wzrost zaangażowania Uczestnika w procesy związane z ochroną danych	Test teoretyczny
Uczestnik identyfikuje, analizuje i zarządza ryzykiem w organizacji	dokumentowanie procesów i procedur dotyczących zarządzania ryzykiem w organizacji	Test teoretyczny
Uczestnicy zapewniają zgodność z obowiązującymi przepisami oraz zapewniają ochronę danych osobowych swoich klientów i pracowników	przestrzeganie przepisów dotyczących ochrony danych osobowych, w tym polityka prywatności i procedury zapewniające bezpieczeństwo danych	Test teoretyczny
Uczestnik umiejętnie zarządza danymi osobowymi, w tym ich zbieraniem, przechowywaniem, przetwarzaniem i usuwaniem, co prowadzi do sprawniejszej i bardziej efektywnej organizacji działań związanych z przetwarzaniem danych	umiejętności techniczne do przechowywania, przetwarzania i usuwania danych osobowych zgodnie z obowiązującymi standardami i przepisami prawnymi	Test teoretyczny
Uczestnik definiuje podstawowe zagrożenia dla systemów IT i OT oraz umiejętnie identyfikuje potencjalne luki w zabezpieczeniach	umiejętna ocena poziomu zabezpieczeń w systemach IT i OT oraz odpowiednie środki zaradcze w celu zapobiegania atakom cybernetycznym	Test teoretyczny
Uczestnik identyfikuje potencjalne zagrożenia, takie jak ataki hakerskie, phishing czy kradzież tożsamości, oraz podejmować odpowiednie działania w celu ich zapobieżenia	Stosowanie zasad bezpiecznego korzystania z internetu i ostrożności podczas korzystania z urządzeń elektronicznych	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

Efekty uczenia się podzielone są na wiedzę, umiejętności oraz kompetencje społeczne nabyte w procesie uczenia się.

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

Kryteria weryfikacji zostały określone jako jednoznaczne, realne oraz możliwe do zweryfikowania. Kryteria doprecyzowują efekty uczenia się, a podczas walidacji pomogą ocenić czy dany efekt został osiągnięty.

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

W ramach jednego dostawcy Zakładów Badań i Atestacji ZETOM im. prof. F. Stauba w Katowicach Sp. z o.o. zapewniamy drugą osobę do przeprowadzenia walidacji niż do procesu kształcenia.
Osobą prowadząca jest Sabina Tatarczyk a osobą prowadzącą walidacje usługi jest Mariusz Malicki.

Program

I.

1. Atrybuty bezpieczeństwa informacji oraz systemów zawierających informacje.
2. System Zarządzania Bezpieczeństwem Informacji – zbiór norm z rodziny ISO 27000.
3. Model systemu zarządzania bezpieczeństwem informacji wg ISO/IEC 27001.
4. Zarządzanie ryzykiem jako determinanta bezpieczeństwa informacji. Zarządzanie ryzykiem bezpieczeństwa informacji zgodnie z wytycznymi ISO 27005.
5. Podstawowe regulacje prawne z zakresu ochrony danych osobowych.

II.

1. RODO – kogo dotyczy, główny cel, podstawowe terminy i definicje, zasady ochrony danych osobowych.
2. Zgodność z prawem przetwarzania danych osobowych.
3. Identyfikacja zagrożeń i analiza ryzyka naruszenia danych – podejście oparte na ryzyku, metoda szacowania ryzyka, zarządzanie ryzykiem naruszenia ochrony informacji zawierających dane osobowe.
4. Obowiązki administratora danych osobowych.
5. Dokumentacja RODO: upoważnienia, realizacja obowiązku informacyjnego, umowy powierzenia przetwarzania danych osobowych.

III.

1. Dokumentacja RODO: rejestr czynności przetwarzania, rejestr kategorii czynności przetwarzania, rejestr naruszeń bezpieczeństwa danych, zbiory zasad postępowania, polityka, procedury.
2. Doskonalenie systemu ochrony danych osobowych jako proces ciągły: szkolenia, bieżące wdrażanie wytycznych i rekomendacji PUODO, audyt i działania poaudytowe.
3. Systemy IT i OT – zabezpieczenia.
4. Zasady cyberbezpieczeństwa. Raport Europejskiej Agencji ds. Cyberbezpieczeństwa (**ENISA**) – główne rodzaje zagrożeń i trendy w ich rozwoju.
5. Najważniejsze wskazówki dotyczące zapewnienia cyberbezpieczeństwa podczas pracy zdalnej i hybrydowej.
6. Skala cyberzagrożeń – Cyfrowa Polska Raport: Cyberbezpieczeństwo w Polsce.

Harmonogram

Liczba przedmiotów/zajęć: 16

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 16 Atrybuty bezpieczeństwa informacji oraz systemów zawierających informacje	Sabina Tatarczyk	09-09-2024	08:00	09:30	01:30
2 z 16 Atrybuty bezpieczeństwa informacji oraz systemów zawierających informacje	Sabina Tatarczyk	09-09-2024	09:30	11:00	01:30
3 z 16 Model systemu zarządzania bezpieczeństwem informacji wg ISO/IEC 27001	Sabina Tatarczyk	09-09-2024	11:00	12:30	01:30
4 z 16 Zarządzanie ryzykiem jako determinanta bezpieczeństwa informacji. Zarządzanie ryzykiem bezpieczeństwa informacji zgodnie z wytycznymi ISO 27005	Sabina Tatarczyk	09-09-2024	12:30	13:15	00:45
5 z 16 Podstawowe regulacje prawne z zakresu ochrony danych osobowych	Sabina Tatarczyk	09-09-2024	13:15	14:15	01:00
6 z 16 RODO – kogo dotyczy, główny cel, podstawowe terminy i definicje, zasady ochrony danych osobowych	Sabina Tatarczyk	10-09-2024	08:00	09:30	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
7 z 16 Zgodność z prawem przetwarzania danych osobowych	Sabina Tatarczyk	10-09-2024	09:30	11:00	01:30
8 z 16 Identyfikacja zagrożeń i analiza ryzyka naruszenia danych – podejście oparte na ryzyku, metoda szacowania ryzyka, zarządzanie ryzykiem naruszenia ochrony informacji zawierających dane osobowe	Sabina Tatarczyk	10-09-2024	11:00	12:30	01:30
9 z 16 Obowiązki administratora danych osobowych	Sabina Tatarczyk	10-09-2024	12:30	13:15	00:45
10 z 16 Dokumentacja RODO: upoważnienia, realizacja obowiązku informacyjnego, umowy powierzenia przetwarzania danych osobowych	Sabina Tatarczyk	10-09-2024	13:15	14:15	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
11 z 16 Dokumentacja RODO: rejestr czynności przetwarzania, rejestr kategorii czynności przetwarzania, rejestr naruszeń bezpieczeństwa danych, zbiory zasad postępowania, polityka, procedury	Sabina Tatarczyk	11-09-2024	08:00	09:30	01:30
12 z 16 Doskonalenie systemu ochrony danych osobowych jako proces ciągły: szkolenia, bieżące wdrażanie wytycznych i rekomendacji PUODO, audyt i działania poaudytowe	Sabina Tatarczyk	11-09-2024	09:30	11:00	01:30
13 z 16 Systemy IT i OT – zabezpieczenia	Sabina Tatarczyk	11-09-2024	11:00	11:45	00:45
14 z 16 Zasady cyberbezpieczeństwa. Raport Europejskiej Agencji ds. Cyberbezpieczeństwa (ENISA) – główne rodzaje zagrożeń i trendy w ich rozwoju	Sabina Tatarczyk	11-09-2024	11:45	12:30	00:45
15 z 16 Najważniejsze wskazówki dotyczące zapewnienia cyberbezpieczeństwa podczas pracy zdalnej i hybrydowej	Sabina Tatarczyk	11-09-2024	12:30	13:15	00:45

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
16 z 16 Skala cyberzagrożeń – Cyfrowa Polska Raport: Cyberbezpieczeństwo w Polsce	Sabina Tatarczyk	11-09-2024	13:15	14:15	01:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 350,50 PLN
Koszt przypadający na 1 uczestnika netto	4 350,00 PLN
Koszt osobogodziny brutto	222,94 PLN
Koszt osobogodziny netto	181,25 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Sabina Tatarczyk

Zarządzanie, komunikacja, rozwój osobisty, coaching, optymalizacja, efektywność. Specjalista w zakresie zarządzania projektami w tym o charakterze B+R. Trener. Doświadczenie w prowadzeniu szkoleń miękkich i coachingu dla środowiska biznesu, kadry samorządowej, pracowników instytucji publicznych, liderów/ek społecznych, pracowników/czek organizacji non-profit. W okresie ostatnich trzech lat przeprowadziła ponad 350 h szkoleń/warsztatów między innymi z motywowania pracowników, zarządzania zespołem, zarządzania relacjami z klientem, kształtowaniem wizerunku-orientacja strategiczna, marketingu i sprzedaży w gospodarce cyfrowej, negocjacje, budowanie modelu biznesu w oparciu o założenia zrównoważonego rozwoju oraz społecznej odpowiedzialności biznesu (ISO 26000).
Wieloletnie doświadczenie zawodowe w organie inspekcyjnym, w tym jako audytor wewnętrzny oraz zastępca kierownika ds. zarządzania jakością (PN-EN ISO/IEC 17020). Nauczyciel akademicki, Inspektor ochrony danych osobowych , Audytor wiodący systemu zarządzania bezpieczeństwem informacji wg ISO/IEC 27001. wykształcenie wyższe II stopnia: mgr socjologii Prowadzenie działalności gospodarczej w zakresie doradczo-szkoleniowym oraz obsługa małych i średnich przedsiębiorstw

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymują materiały szkoleniowe w formie skryptu.

Informacje dodatkowe

Ujęte godziny szkoleniowe są godzinami dydaktycznymi tzn 1h dydaktyczna = 1h lekcyjna(45 min)

Harmonogram zawiera przerwy.

Przerwy ustalne zgodnie z potrzebą Uczestników.

Adres

ul. ks. bpa Herberta Bednorza 17
40-384 Katowice
woj. śląskie

Kontakt

Agnieszka Odrobińska

E-mail agnieszka.odrobinska@zetom.eu
Telefon (+48) 882 062 292