Możliwość dofinansowania

Bezpieczeństwo cyfrowe - kompetencje w zakresie cyfryzacji (poziom podstawowy)

Numer usługi 2024/11/11/44943/2405678

2 643,27 PLN brutto
2 149,00 PLN netto
188,81 PLN brutto/h
153,50 PLN netto/h

RnD.Aero Spółka z Ograniczoną Odpowiedzialnością

★★★★★

Łańcut / stacjonarna
Usługa szkoleniowa
14 h
28.01.2025 do 31.01.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Usługa skierowana jest do całego personelu firm od kadry menadżerskiej i właścicielska/współwłaścicielska po pracowników biurowych. Osoby te powinny posiadać podstawowe kompetencje i wiedzę o obsłudze komputerów i internetu.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	8
Data zakończenia rekrutacji	24-01-2025
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	14
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

Celem podstawowego szkolenia jest przygotowanie do zidentyfikowania i zrozumienia przez uczestników zróżnicowanych źródeł zagrożeń ataków cyfrowych oraz umiejętność wyboru i stosowania zasad zabezpieczeń technicznych i organizacyjnych w celu przeciwdziałania atakom i/lub łagodzenia ich skutków.

Przygotowuje do: budowania świadomości osób przetwarzających informacje,opracowywania/weryfikowania zasad bezpieczeństwa danych,nadzorowania ustanawiania,wdrażania, utrzymania i ciągłego doskonalenia SZBI

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik posługuje się wiedzą, znajomością i interpretacją wymagań normy ISO 27001	Charakteryzuje i rozróżnia poszczególne punkty normy	Test teoretyczny
	Omawia, uzasadnia i charakteryzuje cele i zasady Systemu Zarządzania Bezpieczeństwem Informacji	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, wydawany certyfikat zawiera opis efektów uczenia się.

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

Tak, certyfikat zawiera sformułowanie o sposobie przeprowadzenia walidacji.

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

Tak, certyfikat zawiera sformułowanie o zastosowaniu rozwiązań zapewniających rozdzielność procesów kształcenia i szkolenia od waliacji.

Program

1. Wstęp.

2. Wprowadzenie.

a. Źródła zagrożeń i ataków dotyczące cyberbezpieczeństwa w firmie(wynikających między innymi ze stosowania nowych rozwiązań cyfrowych, w tym algorytmów sztucznej inteligencji, przetwarzania w chmurze, rozwiązań mobilnych)

b. Stosowanie odpowiednich zabezpieczeń przed atakami w tym podstawy zabezpieczania przesyłania danych w przedsiębiorstwie i w całym łańcuchu wartości

c. Zarządzanie i szacowanie ryzyka w bezpieczeństwie informacji / bezpieczeństwie cyfrowym w oparciu o ISO/IEC 27005

d. Regulacje prawne z zakresu ochrony i przetwarzania danych oraz podstaw bezpieczeństwa cyfrowego w przedsiębiorstwie

e. Modele zabezpieczeń oprogramowania

f. Cykl PDCA. Podejście procesowe. Nastawienie na osiągnięcie celów. Monitorowanie i doskonalanie w oparciu o uzyskane wyniki

g. Norma ISO 9001 - podstawowe informacje

h. Norma ISO/IEC 27005 Zarządzanie ryzykiem bezpieczeństwa informacji - wymagania, rola i charakterystyka

3. Omówienie wymagań ISO/IEC 27001 - w zakresie Systemu Zarządzania Bezpieczeństwem informacji

a. Kontekst Organizacyjny

b. Przywództwo. Polityka Bezpieczeństwa Informacji. Role i Odpowiedzialność.

c. Planowanie Systemu Zarządzania Bezpieczeństwem Informacji

d. Wsparcie Systemu Zarządzania Bezpieczeństwem Informacji

e. Realizacja Systemu Zarządzania Bezpieczeństwem Informacji

f. Monitorowanie Systemu Zarządzania Bezpieczeństwem Informacji

g. Ciągłe Doskonalanie

4. Omówienie sposobów zapewnienia bezpieczeństwa informacji zgodnie z Załącznikiem A do ISO/IEC 27001:2022.

a. Polityki Bezpieczeństwa Informacji

b. Organizacja Zabezpieczenia Informacji

c. Bezpieczeństwo Zasobów Ludzkich

d. Zarządzanie

e. Kontrola Dostępu

f. Kryptografia

g. Bezpieczeństwo fizyczne i środowiskowe

h. Bezpieczeństwo operacji

i. Bezpieczeństwo Komunikacji

j. Uzyskanie dostepu, rozwój i utrzymanie systemu

k. Relacje z dostawcami

l. Zarzadzanie incydentami związanymi z bezpieczeństwem informacji

m. Aspekty bezpieczeństwa informacji w zarządzaniu ciagłością biznesu

n. Zgodność

5.Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji.

a. Polityki

b. Procedury i instrukcje w tym przykład metodologii szacowania i zarządzania zidentyfikowanym ryzykiem

c. Zapisy z realizacji Systemu Zarządzania Bezpieczeństwem Informacji w tym przykład analizy zabezpieczeń systemów teleinformatycznych

6. Egzamin

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	2 643,27 PLN
Koszt przypadający na 1 uczestnika netto	2 149,00 PLN
Koszt osobogodziny brutto	188,81 PLN
Koszt osobogodziny netto	153,50 PLN

Prowadzący

Liczba prowadzących: 2

1 z 2

Łukasz Rachfał

Absolwent studiów inżynierskich i magisterskich Politechniki Rzeszowskiej na kierunku Zarządzanie i Inżynieria Produkcji, o specjalności Systemy Zapewnienia Jakości Produkcji.

Odbyte szkolenia Audytora wewnętrznego ISO9001 oraz lotniczej normy z serii AS9110. Praktyczna wiedza i doświadczenie zdobyte podczas audytów wewnętrznych, zewnętrznych oraz klientów.

Doświadczenie praktyczne zdobyte w licznych projektach realizowanych dla firm z branży lotniczej, medycznej oraz informatycznej. Doświadczenie w pracy z firmami projektującymi, produkcyjnymi oraz handlowymi.
Udział w wielu projektach:
- cyfryzacji procesów technologicznych i wdrożenie technologii Przemysłu 4.0
- wdrożeniowych ISO 9001 i ISO 27001
- utrzymanie Systemów Zarządzania Jakością wg ISO9001 oraz AS9100 i AS9120
- utrzymanie Systemów Zarządzania Bezpieczeństwem Informacji wg ISO27001
- przeprowadzanie szkoleń z zakresu Systemów Jakości oraz
Kontroli Jakości
Wiedza i umiejętności z zakresu objętym szkoleniem oraz ocena umiejętności instruktora została pozytywnie zweryfikowane przez Kierownictwo zgodnie z procedurami wdrożonego Systemu Zarządzania Jakości ISO9001. Trener posiada co najmniej 120 godzin doświadczenia w prowadzeniu szkoleń o podobnej tematyce dla osób dorosłych w ostatnich dwóch latach (24 miesiącach) wstecz od dnia rozpoczęcia szkolenia.

2 z 2

Piotr Mróz

Blisko 20 lat doświadczenia w zarządzaniu zespołami, projektami oraz przedsiębiorstwami. W tym ponad 10 lat w branży lotniczej. Praktyczna znajomość organizacji projektujących i produkujących Part 21 oraz obsługowych Part M/145/CAO jak i szkoleniowych Part 66/147 zdobyta podczas pracy na stanowiskach między innymi takich jak: Inżynier Jakości, Kierownik Projektów, Kierownik Jakości, Business Development Manager oraz Managing director. Blisko 10 lat doświadczenia w zarządzaniu bezpieczeństwem. Wykształcenie wyższe zdobyte na Politechnice Rzeszowskiej im. I. Łukasiewicza. Wiedza i umiejętności z zakresu objętym szkoleniem oraz ocena umiejętności instruktora została pozytywnie zweryfikowane przez Kierownictwo zgodnie z procedurami wdrożonego Systemu Zarządzania Jakości ISO9001. Trener posiada co najmniej 120 godzin doświadczenia w prowadzeniu szkoleń o podobnej tematyce dla osób dorosłych w ostatnich dwóch latach (24 miesiącach) wstecz od dnia rozpoczęcia szkolenia.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy uczestnik pierwszego dnia otrzyma komplet materiałów w postaci eletronicznej.

Każdy z uczestników będzie miał dostęp do materiałów ćwiczeniowych

Informacje dodatkowe

Bezpieczeństwo cyfrowe - kompetencje w zakresie cyfryzacji to 14 godzin lekcyjnych, w tym ponad 13 godzin lekcyjnych na zdobywanie wiedzy, umiejętności i kompetencji oraz 30 minut przeznaczonych na egzamin w formie testu wiedzy na temat podstawowych zagadnień dotyczących cyberbezpieczeństwa.

1 godzina lekcyjna to 45 minut, 14 godzin lekcyjnych(14 godzin lekcyjnych x 45minut = 630 minut = 10,5 godzin zegarowych).

Warunkiem uzyskania zaświadczenia jest uczestnictwo, w co najmniej 80% zajęć usługi rozwojowej oraz pozytywna ocena z egzaminu sprawdzającego osiągnięte efekty usługi rozwojowej.

Adres

Łańcut
Łańcut
woj. podkarpackie

Kontakt

Piotr Mróz

E-mail biuro@rndaero.com
Telefon (+48) 502 704 605