Możliwość dofinansowania

Cyberbezpieczeństwo i bezpieczeństwo informacji w przedsiębiorstwie z branży lotniczej

Numer usługi 2025/01/30/44943/2531687

5 043,00 PLN brutto
4 100,00 PLN netto
210,13 PLN brutto/h
170,83 PLN netto/h

RnD.Aero Spółka z Ograniczoną Odpowiedzialnością

★★★★★

zdalna w czasie rzeczywistym
Usługa szkoleniowa
24 h
16.06.2025 do 18.06.2025

Informacje podstawowe

Kategoria	Biznes / Zarządzanie przedsiębiorstwem
Sposób dofinansowania	wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Grupę docelową usługi stanowi kadra menadżerska oraz pracownicy mikro, małych i średnich przedsiębiorstw z branży lotniczej chcący nabyć wiedzę i umiejętności dotyczące identyfikacji źródeł zagrożeń ataków cyfrowych, zapewnienia i zarządzania bezpieczeństwem informacji oraz wyboru i stosowania zasad zabezpieczeń technicznych w organizacyjnych w celu przeciwdziałania atakom i/lub łagodzenia ich skutków.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	7
Data zakończenia rekrutacji	09-06-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
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

Usługa "Cyberbezpieczeństwo i bezpieczeństwo informacji w przedsiębiorstwie z branży lotniczej" prowadzi do prawidłowej identyfikacji źródeł zagrożeń ataków cyfrowych, zapewnienia i zarządzania bezpieczeństwem informacji

oraz stosowania odpowiednich zabezpieczeń technicznych w organizacji działającej w branży lotniczej w celu przeciwdziałania atakom lub łagodzenia ich skutków.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik posługuje się wiedzą z zakresu cyberbezpieczeństwa w organizacji	Potrafi zidentyfikować potencjalne zagrożenia cybernetyczne, takie jak phishing, malware, ransomware czy ataki socjotechniczne.	Test teoretyczny
	Zna i przestrzega obowiązujących procedur oraz polityk dotyczących cyberbezpieczeństwa.	Test teoretyczny
	Potrafi prawidłowo zgłaszać i reagować na podejrzane zdarzenia oraz zna procedury reagowania na incydenty bezpieczeństwa.	Test teoretyczny
Uczestnik posługuje się wiedzą, znajomością i interpretacją wymagań normy ISO/IEC 27001 dotyczącymi cyberbezpieczeństwa	potrafi wskazać cel i zakres normy oraz jej znaczenie dla cyberbezpieczeństwa w organizacji.	Test teoretyczny
	Zna kluczowe sekcje normy, w tym kontekst organizacji, przywództwo, planowanie, wsparcie, działanie, ocenę wyników i doskonalenie.	Test teoretyczny
	Potrafi wyjaśnić i zastosować odpowiednie środki bezpieczeństwa z Załącznika A normy ISO/IEC 27001 w kontekście cyberbezpieczeństwa.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik prawidłowo interpretuje wymagania prawne z obszaru Ochrony Polityki Bezpieczeństwa Informacji	Potrafi wymienić i omówić podstawowe akty prawne regulujące ochronę informacji (np. RODO, Ustawa o Krajowym Systemie Cyberbezpieczeństwa, Ustawa o ochronie danych osobowych, ISO/IEC 27001).	Test teoretyczny
	Potrafi wyjaśnić, jakie obowiązki nakładają przepisy prawne na organizację w zakresie ochrony polityki bezpieczeństwa informacji.	Test teoretyczny
	Potrafi klasyfikować informacje zgodnie z przepisami prawnymi i polityką organizacji (np. dane osobowe, informacje niejawne, tajemnice przedsiębiorstwa).	Test teoretyczny
	Potrafi ocenić, czy wdrożone polityki i procedury bezpieczeństwa spełniają wymagania prawne oraz zalecać ich aktualizację.	Test teoretyczny
Uczestnik planuje, definiuje i wdraża sposoby zabezpieczeń w celu ochrony informacji	Potrafi przeprowadzić ocenę ryzyka oraz zidentyfikować potencjalne zagrożenia dla bezpieczeństwa informacji.	Test teoretyczny
	Potrafi dobrać odpowiednie techniczne, organizacyjne i proceduralne środki zabezpieczeń dostosowane do poziomu ryzyka.	Test teoretyczny
	Definiuje i implementuje zasady nadawania, przeglądu oraz odbierania uprawnień do systemów i zasobów informacyjnych.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik prawidłowo klasyfikuje zagrożenia bezpieczeństwa informacji i cyberbezpieczeństwa	Potrafi wymienić i rozróżnić zagrożenia fizyczne, techniczne, organizacyjne oraz socjotechniczne związane z bezpieczeństwem informacji.	Test teoretyczny
	Potrafi zidentyfikować najczęstsze cyberzagrożenia, takie jak: phishing, ransomware, ataki typu Man-in-the-Middle (MITM), złośliwe oprogramowanie, exploitowanie luk w systemach.	Test teoretyczny
	Potrafi ocenić, w jaki sposób jedno zagrożenie może prowadzić do kolejnych (np. wyciek danych z phishingu prowadzący do szerszego ataku na organizację).	Test teoretyczny
Uczestnik charakteryzuje i prawidłowo definiuje System Bezpieczeństwa Informacji w lotnictwie oraz Bezpieczeństwo danych wrażliwych i danych osobowych	potrafi wymienić i wyjaśnić kluczowe regulacje dotyczące bezpieczeństwa informacji w lotnictwie (np. ICAO, EASA, IATA, ISO/IEC 27001, DO-326A).	Test teoretyczny
	Potrafi poprawnie zdefiniować i omówić kluczowe elementy SZBI stosowanego w branży lotniczej.	Test teoretyczny
	Potrafi określić, kiedy i w jaki sposób należy zgłosić naruszenie ochrony danych odpowiednim organom (np. UODO, EASA, IATA).	Test teoretyczny
	Potrafi w klarowny sposób wyjaśnić zagrożenia związane z bezpieczeństwem informacji i cyberbezpieczeństwem, dostosowując język do poziomu wiedzy zespołu.	Obserwacja w warunkach symulowanych
Uczestnik w sposób prawidłowy i zrozumiany komunikuje wśród swojego zespołu zagrożenia bezpieczeństwa informacji i cyberbezpieczeństwa	Podaje rzeczywiste przypadki zagrożeń (np. ataki phishingowe, ransomware, wycieki danych) i omawia ich konsekwencje.	Obserwacja w warunkach symulowanych
	Członkowie zespołu potrafią poprawnie powtórzyć kluczowe informacje i zastosować je w praktyce.	Obserwacja w warunkach symulowanych

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

Uczestnicy otrzymają certyfikat ukończenia szkolenia, który 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, dokument potwierdza, że walidacja została przeprowadzone w oparciu o zdefiniowane kryteria weryfikacji.

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

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

Program

Szkolenie adresowane jest do pracowników posiadających podstawową wiedzę i doświadczenie z zakresu cyberbezpieczeństwa oraz bezpieczeństwa informacji w branży lotniczej.

Zakres tematyczny usługi obejmuje:

1. Wstęp.

2. Wprowadzenie.

- 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)
- Stosowanie odpowiednich zabezpieczeń przed atakami w tym podstawy zabezpieczania przesyłania danych w przedsiębiorstwie i w całym łańcuchu wartości
- Zarządzanie i szacowanie ryzyka w bezpieczeństwie informacji / bezpieczeństwie cyfrowym w oparciu o ISO/IEC 27005
- Regulacje prawne z zakresu ochrony i przetwarzania danych oraz podstaw bezpieczeństwa cyfrowego w przedsiębiorstwie
- Modele zabezpieczeń oprogramowania

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

- Kontekst Organizacyjny
- Przywództwo. Polityka Bezpieczeństwa Informacji. Role i Odpowiedzialność.
- Planowanie Systemu Zarządzania Bezpieczeństwem Informacji
- Wsparcie Systemu Zarządzania Bezpieczeństwem Informacji
- Realizacja Systemu Zarządzania Bezpieczeństwem Informacji
- Monitorowanie Systemu Zarządzania Bezpieczeństwem Informacji
- Ciągłe Doskonalanie

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

- Polityki Bezpieczeństwa Informacji
- Organizacja Zabezpieczenia Informacji
- Bezpieczeństwo Zasobów Ludzkich
- Zarządzanie
- Kontrola Dostępu
- Kryptografia
- Bezpieczeństwo fizyczne i środowiskowe
- Bezpieczeństwo operacji
- Bezpieczeństwo Komunikacji
- Uzyskanie dostępu, rozwój i utrzymanie systemu
- Relacje z dostawcami

- Zarzadzanie incydentami związanymi z bezpieczeństwem informacji

5 Zabezpieczenia w Systemie Zarządzania Bezpieczeństwem Informacji w lotnictwie

- Polityka Bezpieczeństwa
- Organizacja bezpieczeństwa
- Zarządzanie aktywami
- Bezpieczeństwo osobowe
- Bezpieczeństwo fizyczne i środowiskowe
- Zarządzanie systemami i sieciami
- Kontrola dostępu
- Rozwój i utrzymanie systemu
- Zarządzanie incydentami
- Zarządzanie ciągłością działania
- Zgodność

6 Ćwiczenia praktyczne obejmujące zagadnienia przedstawione w części teoretycznej

7 Egzamin

Ćwiczenia obejmują podział na grupy w zależności od liczby uczestników (od 2-5), w których realizowane są praktyczne przykłady i studia przypadków. Usługa realizowana jest w godzinach dydaktycznych. Przerwy są wliczane w czas usługi rozwojowej. Zajęcia praktyczne obejmują około 20% czasu usługi rozwojowej.

Harmonogram

Liczba przedmiotów/zajęć: 10

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 10 1. Wstęp.	Karol Urban	16-06-2025	08:30	09:15	00:45
2 z 10 2. Wprowadzenie.	Karol Urban	16-06-2025	09:15	12:00	02:45
3 z 10 3. Omówienie wymagań ISO/IEC 27001 - w zakresie Systemu Zarządzania Bezpieczeństwem informacji.	Karol Urban	16-06-2025	12:30	15:00	02:30
4 z 10 4. Omówienie sposobów zapewnienia bezpieczeństwa informacji zgodnie z Załącznikiem A do ISO/IEC 27001:2022.	Karol Urban	16-06-2025	15:00	16:00	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 10 4. Omówienie sposobów zapewnienia bezpieczeństwa informacji zgodnie z Załącznikiem A do ISO/IEC 27001:2022.	Karol Urban	17-06-2025	08:30	10:30	02:00
6 z 10 5 Zabezpieczenia w Systemie Zarządzania Bezpieczeństwem Informacji w lotnictwie.	Karol Urban	17-06-2025	10:30	12:30	02:00
7 z 10 5 Zabezpieczenia w Systemie Zarządzania Bezpieczeństwem Informacji w lotnictwie.	Karol Urban	17-06-2025	13:00	14:00	01:00
8 z 10 6 Ćwiczenia praktyczne obejmujące zagadnienia przedstawione w części teoretycznej.	Łukasz Rachfał	18-06-2025	08:00	11:30	03:30
9 z 10 6 Ćwiczenia praktyczne obejmujące zagadnienia przedstawione w części teoretycznej.	Łukasz Rachfał	18-06-2025	12:00	14:00	02:00
10 z 10 7 Egzamin.	-	18-06-2025	14:00	14:30	00:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 043,00 PLN
Koszt przypadający na 1 uczestnika netto	4 100,00 PLN
Koszt osobogodziny brutto	210,13 PLN
Koszt osobogodziny netto	170,83 PLN

Prowadzący

Liczba prowadzących: 3

1 z 3

Karol Urban

Posiadam 12 letnie doświadczenie na stanowiskach kierowniczych w branży lotniczej:
- Pełnomocnik ds. ZSZ ISO 900,ISO/IEC 27001, AS 9100
- Kierownik Jakości w Part 21 G POA
- Head of ISM a Part 21J DOA
- Dośiadczenie w pracy w Organizacjach obsługowych EASA Part M/F, EASA Part 145
- Znajomość przepisów technicznych z dziedziny lotnictwa CS-25/FAR-25, CS-23/FAR-25, CS-P
- Znajomość wymgań technicznych dla cyfrowych urządzeń awioniki, w szczególności wymagania w zakresie odporności środowiskowej RTCA DO-160 oraz wymagania dla oprogramowania cyfrowych urządzeń awioniki zgodnie z RTCA DO-178C.
- Doświadczenie w projektach związanych modyfikacją floty (od strony projektowania i produkcji) dla wiodących linii lotniczych, w zakresie schematów malowań oraz wyposażenia kabiny pasażerskiej i kokpitu

W trakcie pracy zawodowej zdobyłem unikalne w skali kraju doświadczenie w projektach w branży lotniczej, w szczególności w obszarze zarządzania jakością oraz certyfikacji wyrobów lotniczych.

Swoje doświadczenie wykorzystałem w świadczeniu usług rozwojowych dla firm z branży lotniczej oraz dla innych przedsiębiorstw, co pozwala mi na dostosowanie prowadzonych szkoleń i realizowanych usług doradczych dokładnie do profilu Państwa przedsiębiorstwa.

2 z 3

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

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
- przeprowadzanie szkoleń z zakresu Systemów Jakości oraz
Kontroli Jakości

3 z 3

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 (2019-obecnie) oraz Managing director (2019-obecnie). Blisko 10 lat doświadczenia w zarządzaniu bezpieczeństwem. Wykształcenie wyższe zdobyte na Politechnice Rzeszowskiej im. I. Łukasiewicza.

Osoba prowadząca usługę rozwojową /osoba walidująca posiada doświadczenie zawodowe i kwalifikacje odpowiednie do rodzaju i zakresu niniejszej usługi, zdobyte w przeciągu ostatnich 5 lat od daty publikacji danej usługi. Wiedza i umiejętności z zakresu objętym szkoleniem oraz ocena umiejętności instruktora została pozytywnie zweryfikowane przez Kierownictwo zgodnie z procedurami wdrożonego Systemu Zarządzania Jakości ISO9001.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy uczestnik pierwszego dnia szkolenia otrzyma komplet materiałów w wersji elektronicznej.

Każdy z uczestników będzie miał dostęp do materiałów ćwiczeniowych.

Warunki techniczne

Usługi wykonywane przez naszą firmę są realizowane za pomocą narzędzi Google Meet lub Jitsi Meet

Dla Google Meet wymagany jest komputer z systemem w najnowszych(i 2 poprzednich) wersjach:

Mac OS X

Windows

Google Chrome

Ubuntu

Linuks dystrybucje oparte na Debianie

Do działania Google Meet wymaga aktualnej wersji jednej z wymienionych niżej przeglądarek:

- Chrome
- Mozilla Firefox
- Microsoft Edge
- Apple Safari.

Microsoft Internet Explorer nie zapewnia obsługi Google Meet i Jitsi Meet.

Do korzystania z Jitsi Meet wymagana jest jedna z najnowszych przeglądarek:

- Chrome
- Firefox
- Safari

Wymagane jest również stabilne połączenie z siecią internet. Zalecana prędkość minimalna to 2MB/s. Wymagane jest

posiadanie mikrofonu i słuchawek(głośników). Zalecane jest posiadanie kamery.

Każdy z uczestników przed usługą otrzyma link umożliwiający połączenie się. Link będzie ważny podczas trwania usługi zgodnie z harmonogramem.

Do przeglądania materiałów wymagany jest oprogramowanie Adobe Acrobat Reader lub inne pozwalające na otwarcie pliku PDF.

Kontakt

Piotr Mróz

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