Możliwość dofinansowania

Cyberbezpieczeństwo w Przedsiębiorstwie

Numer usługi 2026/01/30/154103/3296664

5 800,00 PLN brutto
5 800,00 PLN netto
193,33 PLN brutto/h
193,33 PLN netto/h

FUNDACJA POLSKIE CENTRUM ROZWOJU EDUKACJI

4,9 / 5

251 ocen

Rzeszów / stacjonarna
Usługa szkoleniowa
30 h
13.04.2026 do 29.05.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Usługa szkoleniowa skierowana jest do osób wykonujących pracę zawodową związaną z przetwarzaniem danych osobowych oraz informacji organizacji, w szczególności do: • pracowników i współpracowników organizacji publicznych i prywatnych, • pracowników administracji, kadr, księgowości, sprzedaży, obsługi klienta, sekretariatów i logistyki, • koordynatorów, liderów oraz kierowników zespołów, Szkolenie jest odpowiednie dla uczestników bez specjalistycznej wiedzy technicznej i może być realizowane niezależnie od branży
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	12-04-2026
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	30
Podstawa uzyskania wpisu do BUR	Znak Jakości TGLS Quality Alliance

Cel

Cel edukacyjny

Celem szkolenia jest przygotowanie uczestników do samodzielnego i świadomego działania w obszarze bezpieczeństwa systemów informatycznych wykorzystywanych w przedsiębiorstwie. Uczestnicy zdobędą praktyczne umiejętności w zakresie rozpoznawania zagrożeń cybernetycznych, podejmowania działań zapobiegawczych, reagowania na incydenty bezpieczeństwa oraz minimalizowania ich wpływu na funkcjonowanie organizacji. Po ukończeniu szkolenia uczestnicy będą potrafili stosować zasady ochrony informacji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik zna kluczowe pojęcia związane z bezpieczeństwem informacji i funkcjonowaniem cyberprzestrzeni. Rozumie rolę ochrony danych w zapewnieniu ciągłości działania przedsiębiorstwa. Posiada wiedzę na temat podstawowych norm i standardów zarządzania bezpieczeństwem informacji, w tym międzynarodowych standardów bezpieczeństwa.	Uczestnik potrafi rozpoznawać zagrożenia wynikające z braku lub nieprawidłowego stosowania zasad bezpieczeństwa informacji. Umie opracować podstawowe zasady i procedury bezpieczeństwa oraz wdrażać je w środowisku organizacyjnym. Potrafi zidentyfikować incydent bezpieczeństwa i zna zasady postępowania oraz zgłaszania takich zdarzeń.	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

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

TAK

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

TAK

Program

Program szkolenia

1.1. Podstawy bezpieczeństwa informacji

Kluczowe pojęcia i zakres cyberbezpieczeństwa

Pojęcie bezpieczeństwa informacji i cyberprzestrzeni.

Rola cyberbezpieczeństwa w funkcjonowaniu i ciągłości działania przedsiębiorstw.

Zarządzanie bezpieczeństwem w organizacji

Znaczenie zasad i procedur bezpieczeństwa w ochronie danych.

Opracowywanie, wdrażanie i aktualizacja polityk bezpieczeństwa informacji.

Zdarzenia i incydenty bezpieczeństwa

Charakterystyka incydentów naruszających bezpieczeństwo systemów IT.

Przykładowe sytuacje zagrożeń oraz zasady reagowania i raportowania.

Standardy i dobre praktyki bezpieczeństwa

Omówienie wybranych norm i wytycznych bezpieczeństwa informacji.

Korzyści organizacyjne wynikające z wdrażania standardów bezpieczeństwa.

1.2. Regulacje prawne i odpowiedzialność (1 godzina)

Odpowiedzialność pracowników w obszarze IT

Skutki prawne nieuprawnionego dostępu do systemów informatycznych.

Odpowiedzialność za ujawnienie informacji i zaniedbania w zakresie ochrony danych.

Ochrona danych osobowych w praktyce

Podstawowe obowiązki wynikające z przepisów o ochronie danych osobowych.

Zasady bezpiecznego przetwarzania danych klientów i pracowników.

2.1. Ataki ukierunkowane na użytkownika – socjotechnika

Mechanizmy manipulacji i wpływu

Najczęściej stosowane techniki wywierania wpływu i wyłudzania informacji.

Sygnały świadczące o próbie ataku socjotechnicznego.

Pozyskiwanie informacji przez atakujących

Dane udostępniane świadomie i nieświadomie w środowisku cyfrowym.

Ograniczanie śladów informacyjnych w Internecie i mediach społecznościowych.

Postępowanie w przypadku prób manipulacji

Zasady reagowania na zagrożenia socjotechniczne.

Zadania praktyczne z zakresu identyfikowania prób wyłudzeń.

2.2. Zagrożenia techniczne dla systemów informatycznych

Rodzaje ataków technicznych

Ataki wykorzystujące sieci bezprzewodowe i urządzenia mobilne.

Fałszywe wiadomości elektroniczne, strony internetowe i komunikatory.

Zabezpieczenia i ochrona systemów

Mechanizmy ochrony działające w czasie rzeczywistym.

Wykrywanie zagrożeń oraz analiza bezpieczeństwa systemów IT.

Zajęcia praktyczne

Symulacje ataków phishingowych i ich analiza.

Ocena podejrzanych wiadomości oraz stron internetowych.

2.3. Bezpieczne korzystanie z zasobów firmowych

Zarządzanie hasłami i uprawnieniami

Zasady tworzenia i przechowywania bezpiecznych haseł.

Kontrola dostępu do zasobów informatycznych organizacji.

Bezpieczeństwo pracy z oprogramowaniem

Bezpieczne korzystanie z poczty elektronicznej i przeglądarek internetowych.

Podstawy ochrony danych – szyfrowanie i certyfikaty bezpieczeństwa.

Ochrona fizyczna zasobów

Zabezpieczanie urządzeń, dokumentów i nośników informacji.

Dodatkowe informacje:

- Szkolenie prowadzone jest w trybie godzin dydaktycznych (45 minut).
- Czas trwania szkolenia: 30 godzin dydaktycznych (plus dodatkowo przerwy).
- Szkolenie będzie prowadzone w grupach maksymalnie 12 osobowych.
- Każda osoba będzie miała przydzielone stanowisko do praktycznych zajęć.
- Kurs prowadzony będzie w formie warsztatowej, zakładającej aktywny udział Uczestników i przeprowadzenie ćwiczeń praktycznych
- Podczas szkolenia przeprowadzane będą regularne weryfikacje postępów oraz ocena osiągnięcia efektów uczenia się poprzez ankiety i testy.

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	5 800,00 PLN
Koszt przypadający na 1 uczestnika netto	5 800,00 PLN

Koszt osobogodziny brutto	193,33 PLN
Koszt osobogodziny netto	193,33 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Jolanta Dyrkacz

trener

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Książka

Informacje dodatkowe

Zajęcia będą realizowane w oparciu o miarę godziny lekcyjnej wynoszącej 45 minut.

Szkolenie będzie realizowane w formie stacjonarnej.

W zależności od czasu, potrzeb będą wykorzystywane różne elementy: ćwiczenia, testy, ankiety i inne.

W efekcie ukończenia kursu Uczestnicy uzyskają zaświadczenie ukończenia kursu, potwierdzający nabycie kompetencji w cyberbezpieczeństwie w Przedsiębiorstwie

Adres

ul. Wincentego Pola 18
35-021 Rzeszów
woj. podkarpackie

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Laboratorium komputerowe

Kontakt

MARTYNA ADAMSKA

E-mail m.adamska@pcre.pl

Telefon (+48) 537 792 855