Możliwość dofinansowania

CENTRUM ANDRZEJ SZOPE SPÓŁKA JAWNA

4,8 / 5

358 ocen

Cyberbezpieczeństwo w organizacji – poziom zaawansowany. Zarządzanie ryzykiem cyfrowym i zielone kompetencje w środowisku pracy

Numer usługi 2026/03/05/162860/3383482

Olsztyn
Usługa szkoleniowa
stacjonarna
18:00 h
13.07.2026 do 14.07.2026

5 200,00 PLN brutto
5 200,00 PLN netto
288,89 PLN brutto/h
288,89 PLN netto/h
261,33 PLN cena rynkowa

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie skierowane jest do osób, które posiadają podstawową wiedzę z zakresu cyberbezpieczeństwa oraz chcą rozwijać kompetencje w zakresie zarządzania bezpieczeństwem informacji w organizacji. W szczególności do: • pracowników administracji publicznej • pracowników biurowych • specjalistów IT • menedżerów i kierowników zespołów • pracowników działów nowych technologii • osób odpowiedzialnych za ochronę danych • właścicieli i pracowników MŚP Szkolenie jest szczególnie rekomendowane dla osób, które ukończyły szkolenie: **„Bądź bezpieczny w sieci – cyberbezpieczeństwo w praktyce”, jednak nie wyklucza się możliwości zapisania na szkolenie osób które deklarują wyższy poziom wiedzy w zakresie podstaw cyberbezpieczeństwa**
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	12-07-2026
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	18

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

Szkolenie przygotowuje uczestników do samodzielnego identyfikowania i analizowania zagrożeń cybernetycznych w organizacji oraz podejmowania działań zwiększających bezpieczeństwo informacji. Uczestnicy zdobywają wiedzę i umiejętności w zakresie oceny poziomu zabezpieczeń, reagowania na incydenty oraz stosowania rozwiązań wspierających zrównoważone i odpowiedzialne wykorzystanie zasobów cyfrowych.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik wyjaśnia zasady zarządzania bezpieczeństwem informacji w organizacji oraz charakteryzuje metody analizy ryzyka cybernetycznego, a także opisuje rolę cyberbezpieczeństwa w zapewnieniu ciągłości działania przedsiębiorstwa i identyfikuje wpływ technologii cyfrowych na środowisko oraz zrównoważony rozwój	uczestnik wskazuje podstawowe elementy zarządzania bezpieczeństwem informacji w organizacji	Test teoretyczny
	opisuje etapy analizy ryzyka cybernetycznego	Test teoretyczny
	wyjaśnia znaczenie cyberbezpieczeństwa dla ciągłości działania organizacji	Test teoretyczny
	wskazuje rozwiązania technologiczne wspierające zrównoważone wykorzystanie zasobów cyfrowych	Test teoretyczny
Uczestnik przeprowadza podstawową analizę ryzyka cybernetycznego, identyfikuje słabe punkty w systemach bezpieczeństwa organizacji, projektuje procedury reagowania na incydenty oraz stosuje narzędzia zabezpieczające dane i systemy informatyczne, w tym rozwiązania ograniczające zużycie zasobów cyfrowych i energii.	uczestnik identyfikuje zagrożenia w przykładowym środowisku pracy	Wywiad swobodny
	wskazuje słabe punkty w systemach bezpieczeństwa organizacji	Wywiad swobodny
	opracowuje schemat postępowania w sytuacji incydentu cybernetycznego	Wywiad swobodny
	dobiera narzędzia zabezpieczające dane i systemy informatyczne	Obserwacja w warunkach rzeczywistych
	wskazuje rozwiązania zwiększające efektywność wykorzystania zasobów cyfrowych	Wywiad swobodny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik podejmuje decyzje w sytuacjach zagrożenia cybernetycznego, współpracuje w zespole przy wdrażaniu procedur bezpieczeństwa oraz stosuje zasady odpowiedzialnego i bezpiecznego korzystania z technologii cyfrowych.	uczestnik analizuje sytuacje problemowe i proponuje właściwe działania	Wywiad swobodny
	aktywnie uczestniczy w ćwiczeniach zespołowych dotyczących bezpieczeństwa informacji	Analiza dowodów i deklaracji
	wskazuje dobre praktyki odpowiedzialnego korzystania z technologii cyfrowych	Analiza dowodów i deklaracji

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

Cyberbezpieczeństwo w organizacji – poziom zaawansowany. Zarządzanie ryzykiem cyfrowym i zielone kompetencje w środowisku pracy

Szkolenie składa się z **2 dni szkoleniowych po 9 godzin dydaktycznych**, w tym **1 godziny walidacji realizowanej w formie zdalnej w czasie rzeczywistym (45 minut)**.

Łączny czas trwania szkolenia wynosi **18 godzin dydaktycznych**, w tym:

- **17 godzin dydaktycznych w formie stacjonarnej**
- **1 godzina dydaktyczna w formie zdalnej w czasie rzeczywistym – walidacja**

Część stacjonarna obejmuje:

- **9 godzin zajęć teoretycznych**
- **8 godzin zajęć praktycznych**

Jedna godzina dydaktyczna trwa **45 minut**.

Szkolenie jest przeznaczone dla osób chcących pogłębić wiedzę z zakresu cyberbezpieczeństwa w organizacji oraz nauczyć się zarządzania ryzykiem cyfrowym, identyfikacji zagrożeń oraz wdrażania procedur bezpieczeństwa informacji w przedsiębiorstwie.

Usługa rozwija również **zielone kompetencje cyfrowe**, w szczególności w zakresie odpowiedzialnego zarządzania zasobami cyfrowymi, ograniczania zużycia energii przez infrastrukturę IT oraz stosowania rozwiązań wspierających zrównoważony rozwój organizacji.

Szkolenie rekomendowane jest dla osób posiadających podstawową wiedzę z zakresu cyberbezpieczeństwa lub które ukończyły szkolenie **„Bądź bezpieczny w sieci – cyberbezpieczeństwo w praktyce”**.

Warunki organizacyjne

Uczestnicy podczas zajęć korzystają z komputerów zapewnionych przez organizatora szkolenia.

Każdy uczestnik dysponuje **indywidualnym stanowiskiem komputerowym**, umożliwiającym samodzielną realizację ćwiczeń i zadań praktycznych.

Stanowiska komputerowe wyposażone są w:

- podstawowe oprogramowanie biurowe
- przeglądarki internetowe (Google Chrome, Mozilla Firefox lub Safari)
- narzędzia wspierające analizę zagrożeń i symulacje cyberataków.

Podczas szkolenia uczestnicy realizują ćwiczenia praktyczne obejmujące m.in.:

- analizę ryzyka cybernetycznego w organizacji
- identyfikację słabych punktów infrastruktury IT
- analizę rzeczywistych scenariuszy cyberataków
- projektowanie procedur reagowania na incydenty bezpieczeństwa
- symulacje cyberataków oraz reakcję na incydenty
- tworzenie podstawowych elementów polityki bezpieczeństwa informacji
- analizę bezpieczeństwa pracy zdalnej i chmurowej
- identyfikację rozwiązań ograniczających zużycie energii i zasobów cyfrowych.

Harmonogram szkolenia

Dzień I

Moduł 1

Wprowadzenie do zarządzania cyberbezpieczeństwem w organizacji

- rola cyberbezpieczeństwa w funkcjonowaniu przedsiębiorstwa
- aktualne zagrożenia cyfrowe w środowisku biznesowym
- wpływ cyberataków na działalność organizacji

Moduł 2

Analiza ryzyka cybernetycznego

- identyfikacja zagrożeń i podatności systemów
- ocena poziomu ryzyka w organizacji
- analiza scenariuszy cyberataków

Moduł 3

Audyt bezpieczeństwa systemów informatycznych

- identyfikacja słabych punktów infrastruktury IT

- ocena poziomu zabezpieczeń w organizacji
- dobre praktyki wzmacniania bezpieczeństwa systemów

Dzień II

Moduł 4

Zarządzanie incydentami cybernetycznymi

- procedury reagowania na incydenty
- minimalizowanie skutków cyberataków
- komunikacja w sytuacjach kryzysowych

Moduł 5

Bezpieczeństwo pracy zdalnej i usług chmurowych

- zagrożenia związane z pracą zdalną
- bezpieczne korzystanie z usług chmurowych
- zarządzanie dostępem do danych

Moduł 6

Cyberbezpieczeństwo a zielone kompetencje

- efektywne zarządzanie infrastrukturą IT
- ograniczanie zużycia energii w systemach cyfrowych
- odpowiedzialne korzystanie z zasobów cyfrowych
- cyberbezpieczeństwo w kontekście zrównoważonego rozwoju organizacji

Moduł 7

Warsztaty praktyczne

- symulacje cyberataków
- analiza przypadków naruszeń bezpieczeństwa
- projektowanie procedur bezpieczeństwa w organizacji

Walidacja

Walidacja efektów uczenia się przeprowadzana jest **w formie stacjonarnej**

Walidacja obejmuje:

- **test teoretyczny** sprawdzający poziom wiedzy (ok. 30 minut)
- **obserwację w warunkach symulowanych**
- **wywiad swobodny**

Warunkiem zaliczenia części teoretycznej jest uzyskanie **minimum 80% prawidłowych odpowiedzi**.

Walidator nie bierze udziału w części edukacyjnej usługi.

Informacje organizacyjne

W ciągu każdego dnia szkoleniowego przewidziane są **trzy przerwy**, 2 przerwy 15-minutowe oraz jedna obiadowa 30 -minutowa które nie wliczają się do czasu trwania usługi.

Cena usługi nie obejmuje kosztów niezwiązanych bezpośrednio z usługą rozwojową, takich jak koszty dojazdu lub zakwaterowania uczestników.

Harmonogram

Liczba pozycji harmonogramu: 0

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 200,00 PLN
Koszt przypadający na 1 uczestnika netto	5 200,00 PLN
Koszt osobogodziny brutto	288,89 PLN
Koszt osobogodziny netto	288,89 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Agnieszka Poniatowska

od 2019 - 2023 - Trener w Centrum Szkoleniowym MS Szkolenia Marlena Sobieska - Ciesielska

ZAKRES SZKOLEŃ:
warsztaty umiejętności psychospołecznych
szkolenia trenerskie dla liderów
budowanie autorytetu trenera
szkolenie z umiejętności i technik trenerskich
budowanie motywacji i zarządzanie zaangażowaniem pracowników
szkolenia interpersonalne i kursy umiejętności osobistych
szkolenia z zakresu rynku pracy
stres, zmęczenie i wypalenie zawodowe
pracownik administracyjno - biurowy
kurs komputerowy - obsługa komputera oraz pakietu Microsoft Office: (600h)
Word,
Excel,
PowerPoint,
Access,

Publisher,
Outlook,
OneNote
Rozwiązywanie problemów
IT Security
negocjacje

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Notatnik, długopis

Prezentacja w formie multimedialnej zostanie wysłana na e-mail Uczestników.

Informacje dodatkowe

Szkolenie trwa 18 godzin dydaktyczne w tym walidacja trwa 45minut.

Szkolenie składa się z 17h dydaktycznych w formie stacjonarnej oraz 1 godziny dydaktycznej w formie stacjonarnej tj. walidacji.

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

W ciągu szkolenia zostały uwzględnione 3 przerwy - 2 po 15 minut i jedna 30 minutowa, które nie są wliczane do czasu trwania usługi.

Koszt szkolenia nie zawiera kosztów dojazdu, wyżywienia i noclegu.

Podstawą do rozliczenia usługi jest wygenerowany z systemu raport umożliwiający identyfikację wszystkich uczestników na walidacji oraz zastosowanego narzędzia.

Uczestnik szkolenia otrzyma zaświadczenie o ukończeniu szkolenia dopiero po pozytywnym wyniku walidacji, który odbędzie się na ostatnich zajęciach. Warunkiem otrzymania zaświadczenia o ukończeniu szkolenia jest pozytywny wynik walidacji końcowej.

Adres

ul. Maurycego Mochnackiego 10/1
10-037 Olsztyn
woj. warmińsko-mazurskie

Szkolenie będzie realizowane w firmie Centrum Nauka Jazdy

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi

Kontakt

KLAUDIA ZEJER

E-mail k.zejer@centrum-osk.pl
Telefon (+48) 664 265 725