



AKADEMIA
PIOTRKOWSKA

Brak ocen dla tego dostawcy

Podstawy cyberbezpieczeństwa i bezpieczeństwa informacji - szkolenie

Numer usługi 2026/03/24/179261/3432171

📍 Piotrków Trybunalski
🏢 Usługa szkoleniowa
📅 stacjonarna
🕒 08:00 h
📅 17.06.2026 do 17.06.2026

800,00 PLN brutto
800,00 PLN netto
100,00 PLN brutto/h
100,00 PLN netto/h
175,56 PLN cena rynkowa ⓘ

Informacje podstawowe

Kategoria

Prawo i administracja / Administracja publiczna

Grupa docelowa usługi

Szkolenie jest skierowane do podmiotów komunalnych realizujących zadania związane z infrastrukturą, obsługą techniczną, administracją i świadczeniem usług publicznych. Usługa jest odpowiednia dla pracowników administracyjnych, technicznych, operacyjnych, pracowników obsługi klienta, osób odpowiedzialnych za obieg dokumentów i informacji, a także dla kadry kierowniczej średniego szczebla oraz osób współpracujących przy utrzymaniu ciągłości działania, ochronie danych, bezpieczeństwie informacji i reagowaniu na incydenty. Szkolenie przeznaczone jest dla osób, które w codziennej pracy korzystają z systemów informatycznych, przetwarzają informacje służbowe, mają styczność z danymi osobowymi lub uczestniczą w przepływie informacji wewnątrz organizacji i w kontaktach z mieszkańcami, kontrahentami oraz instytucjami zewnętrznymi.

Minimalna liczba uczestników

10

Maksymalna liczba uczestników

30

Data zakończenia rekrutacji

16-06-2026

Forma prowadzenia usługi

stacjonarna

Liczba godzin usługi

8

Podstawa uzyskania wpisu do BUR

art. 163 ust. 1 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (t. j. Dz. U. z 2024 r. poz. 1571, z późn. zm.)

Zakres uprawnień

Kursy i szkolenia

Cel

Cel edukacyjny

Usługa przygotowuje do rozpoznawania podstawowych zagrożeń cyberbezpieczeństwa i bezpieczeństwa informacji, stosowania zasad ochrony informacji i danych osobowych, bezpiecznego korzystania z systemów IT oraz podejmowania właściwych działań w sytuacji incydentu, naruszenia lub zakłócenia bezpieczeństwa informacji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Efekt uczenia się 1 Uczestnik charakteryzuje podstawowe pojęcia, zasady i obowiązki związane z cyberbezpieczeństwem, bezpieczeństwem informacji, ochroną danych osobowych oraz bezpiecznym korzystaniem z zasobów teleinformatycznych.	wskazuje podstawowe obowiązki pracownika związane z bezpiecznym korzystaniem z narzędzi cyfrowych i postępowaniem z informacją.	Test teoretyczny
	rozróżnia podstawowe pojęcia, takie jak: cyberbezpieczeństwo, bezpieczeństwo informacji, incydent, naruszenie, dane osobowe;	Test teoretyczny
	wskazuje podstawowe rodzaje zagrożeń dla informacji, użytkowników i organizacji;	Test teoretyczny
	wyjaśnia znaczenie ochrony informacji, danych osobowych oraz stosowania procedur wewnętrznych;	Test teoretyczny
Efekt uczenia się 2 Uczestnik identyfikuje podstawowe zagrożenia dla bezpieczeństwa informacji i ciągłości działania organizacji oraz dobiera adekwatne działania ograniczające ryzyko i skutki incydentów.	wskazuje znaczenie współpracy z przełożonymi, komórką IT oraz innymi osobami odpowiedzialnymi za bezpieczeństwo.	Test teoretyczny
	rozpoznaje przykładowe zagrożenia związane z phishingiem, złośliwym oprogramowaniem, nieuprawnionym dostępem, błędnym obiegiem informacji oraz dezinformacją;	Test teoretyczny
	wskazuje właściwe działania podejmowane po ujawnieniu incydentu, naruszenia lub nieprawidłowości;	Test teoretyczny
	dobiera podstawowe środki organizacyjne i techniczne ograniczające ryzyko;	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Efekt uczenia się 3 Uczestnik stosuje podstawowe zasady bezpiecznego postępowania z informacją oraz właściwej komunikacji w sytuacjach ryzyka, incydentu lub zakłócenia.	• rozpoznaje podstawowe przejawy propagandy i dezinformacji oraz wskazuje ich możliwy wpływ na funkcjonowanie organizacji.	Test teoretyczny
	• wskazuje prawidłowy sposób postępowania z informacjami służbowymi i danymi osobowymi;	Test teoretyczny
	• rozróżnia sytuacje wymagające szczególnej ostrożności oraz właściwe kanały przekazywania informacji; • uczestniczy w rozwiązaniu sytuacji problemowej z uwzględnieniem zasad odpowiedzialności, współpracy i ochrony informacji;	Test teoretyczny Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyrażnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyrażnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyrażnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Szkolenie jest adresowane do podmiotów komunalnych oraz innych organizacji realizujących zadania związane z infrastrukturą, obsługą techniczną, administracją i świadczeniem usług publicznych. Usługa jest odpowiednia dla pracowników administracyjnych, technicznych, operacyjnych, pracowników obsługi klienta, osób odpowiedzialnych za obieg dokumentów i informacji, a także dla kadry kierowniczej średniego szczebla oraz osób współpracujących przy utrzymaniu ciągłości działania, ochronie danych, bezpieczeństwie informacji i reagowaniu na incydenty.

Usługa realizowana jest w formie stacjonarnej i obejmuje 8 godzin dydaktycznych (1 godzina dydaktyczna = 45 minut), w tym 6 godzin zajęć teoretycznych, 1 godzinę zajęć praktycznych oraz 1 godzinę walidacji. Przerwy nie są uwzględnione w czasie trwania usługi.

Ramowy program usługi obejmuje:

- 1. Podstawy cyberbezpieczeństwa i bezpieczeństwa informacji.
- 2. Organizacja systemu cyberbezpieczeństwa oraz regulacje prawne w zakresie bezpieczeństwa informacji.
- 3. Ochrona i wymiana informacji oraz ochrona danych osobowych.
- 4. Zarządzanie bezpieczeństwem informacyjnym.
- 5. Propaganda, dezinformacja i odporność informacyjna organizacji.
- 6. Ćwiczenia praktyczne.
- 7. Walidacja efektów uczenia się – test wiedzy.

Walidacja odbywa się po zakończeniu części dydaktycznej usługi i jest prowadzona w formie testu teoretycznego. Test weryfikuje osiągnięcie wszystkich efektów uczenia się wskazanych w Karcie Usługi. Warunkiem zaliczenia usługi jest uzyskanie pozytywnego wyniku z walidacji.

Harmonogram

Liczba pozycji harmonogramu: 8

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 8 Podstawy cyberbezpieczeństwa i bezpieczeństwa informacji	Jan Zych	17-06-2026	08:00	08:45	00:45
2 z 8 Organizacja systemu cyberbezpieczeństwa oraz regulacje prawne w zakresie bezpieczeństwa informacji	Jan Zych	17-06-2026	08:45	09:30	00:45
3 z 8 Ochrona i wymiana informacji oraz ochrona danych osobowych	Jan Zych	17-06-2026	09:40	10:25	00:45
4 z 8 Ochrona i wymiana informacji oraz ochrona danych osobowych	Jan Zych	17-06-2026	10:25	11:10	00:45

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 8 Zarządzanie bezpieczeństwem informacyjnym	Jan Zych	17-06-2026	11:30	12:15	00:45
6 z 8 Propaganda, dezinformacja i odporność informacyjna organizacji	Jan Zych	17-06-2026	12:15	13:00	00:45
7 z 8 Ćwiczenia praktyczne	Jan Zych	17-06-2026	13:30	14:15	00:45
8 z 8 Walidacja - test końcowy	-	17-06-2026	14:15	15:00	00:45

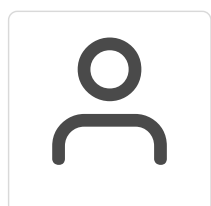
Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	800,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	800,00 PLN
Koszt osobogodziny brutto	100,00 PLN
Koszt osobogodziny netto	100,00 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Jan Zych

Profesor nauk o bezpieczeństwie, specjalista z zakresu adaptacji nowych technologii dla bezpieczeństwa, cyberbezpieczeństwa, kształtowania kompetencji menedżerskich dla bezpieczeństwa, metod i technik doboru pracowników dla sfery bezpieczeństwa, procesów decyzyjnych, inteligentnych systemów wspomagania decyzji, symulacji komputerowych w obszarze

bezpieczeństwa, szkoleniowiec, dydaktyk z wieloletnim doświadczeniem, posiada doświadczenie adekwatne do realizowanej usługi

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymują materiały szkoleniowe obejmujące:

- prezentację tematyczną,
- materiały do ćwiczeń,
- arkusz testowy

Warunki uczestnictwa

Nie są wymagane specjalistyczne kwalifikacje wstępne. Wskazane jest wykonywanie obowiązków zawodowych związanych z funkcjonowaniem organizacji, jej bezpieczeństwem, obsługą procesów operacyjnych, technicznych, administracyjnych lub komunikacyjnych.

Informacje dodatkowe

Szkolenie realizowane jest w formie stacjonarnej. Do przeprowadzenia usługi wymagane jest zapewnienie sali szkoleniowej umożliwiającej pracę warsztatową, projektora lub monitora, dostępu do prezentacji multimedialnej, materiałów szkoleniowych oraz warunków do przeprowadzenia ćwiczeń i walidacji efektów uczenia się.

Informacja o nabywanych kompetencjach:

Usługa prowadzi do nabycia kompetencji w zakresie podstaw bezpieczeństwa organizacyjnego i zarządzania kryzysowego, obejmujących wiedzę, umiejętności oraz kompetencje społeczne związane z rozpoznawaniem zagrożeń, reagowaniem na incydenty, współpracą w sytuacjach zakłóceń i stosowaniem podstawowych zasad komunikacji kryzysowej, z uwzględnieniem wpływu cyfryzacji procesów, bezpieczeństwa informacji oraz uwarunkowań wynikających z zielonej transformacji i racjonalnego gospodarowania zasobami.

Adres

ul. Juliusza Słowackiego 11114/118

97-300 Piotrków Trybunalski

woj. łódzkie

Zajęcia odbywają się w budynku B Akademii Piotrkowskiej przy ul. J. Słowackiego 114/118 w Piotrkowie Trybunalskim

Udogodnienia w miejscu realizacji usługi

- Wi-fi
- bezpłatny parking dla uczestników, udogodnienia dla osób z niepełnosprawnościami

Kontakt

PAULINA ŁAZUTKA-GAWĘDA

E-mail paulina.lazutka-gaweda@apt.edu.pl



Telefon (+48) 447 327 418