



Europejska Agencja
Rozwoju Mirosław
Kopik

★★★★★ 5,0 / 5

3 857 ocen

ZAGROŻENIA CYBERNETYCZNE I BEZPIECZEŃSTWO INFORMACJI W ORGANIZACJI - szkolenie

Numer usługi 2026/08/12/27209/3743101

- 📄 Usługa szkoleniowa
- 📺 zdalna w czasie rzeczywistym
- 👥 Zajęcia grupowe
- 🕒 08:00 h
- 📅 05.11.2026 do 05.11.2026

2 200,00 PLN brutto
2 200,00 PLN netto
275,00 PLN brutto/h
275,00 PLN netto/h
261,33 PLN cena rynkowa ⓘ

Informacje podstawowe

Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

Grupa docelowa usługi

Właściciele firm, menadżerowie, kierownicy działów handlowych, liderzy, handlowcy, przedstawiciele handlowi, sprzedawcy, kadra zarządzająca handlem, pracownicy działu obsługi klienta, technicy, doradcy, marketerzy, specjaliści ds. logistyki, handlu, obsługi klienta, księgowości, rozliczeń, finansów, produkcji, zakupów, rozwoju, obsługi biura, obsługi informatycznej, menadżerowie produktów i projektów; właściciele i pracownicy instytucji ochrony zdrowia, osoby prowadzące działalność z zakresu opieki zdrowotnej, organizujące i zarządzające ochroną zdrowia, promujące zdrowie, pracownicy urzędów gminnych, miejskich i wiejskich, właściciele i pracownicy ośrodków sportu i rekreacji, ośrodków kultury, sztuki, pracownicy instytucji oświatowych, pracownicy jednostek samorządu terytorialnego oraz inne osoby zainteresowane zdobyciem nowych kompetencji, osoby, które chcą doskonalić umiejętności, aby zapobiec utracie zatrudnienia, osoby poszukujące nowych możliwości zawodowych.

Minimalna liczba uczestników

4

Maksymalna liczba uczestników

24

Data zakończenia rekrutacji

04-11-2026

Forma prowadzenia usługi

zdalna w czasie rzeczywistym

Podstawa uzyskania wpisu do BUR

Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Usługa przygotowuje do: praktycznego stosowania wymogów prawnych i procedur wewnętrznych, sprawnego udziału w systemie bezpieczeństwa informacji organizacji zgodnie z przepisami RODO, UODO, KRI, KSC oraz ustawą o ochronie sygnalistów; rozpoznawania i neutralizowania zagrożeń cybernetycznych; zaawansowanego zarządzania tożsamością i dostępem; prawidłowego reagowania na incydenty bezpieczeństwa; bezpiecznego przetwarzania danych osobowych i poufnych – stosowanie odpowiednich zabezpieczeń.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje zasady bezpieczeństwa informacji oraz podstawowe elementy systemu ochrony informacji w organizacji. Stosuje zasady zarządzania dostępem do zasobów organizacji, w tym zasadę minimalnych uprawnień.	Wskazuje elementy triady PID: poufność, integralność i dostępność.	Test teoretyczny
	Rozróżnia autentyczność i niezaprzeczalność informacji.	Test teoretyczny
	Określa rolę polityk i procedur bezpieczeństwa w organizacji.	Test teoretyczny
	Wskazuje właściwy zakres uprawnień dla określonego stanowiska.	Test teoretyczny
	Wskazuje zasady bezpiecznego onboardingu i offboardingu.	Test teoretyczny
Stosuje zasady bezpiecznego zarządzania hasłami, uwierzytelnianiem wieloskładnikowym oraz menedżerami haseł.	Identyfikuje cechy bezpiecznego hasła.	Test teoretyczny
	Rozpoznaje błędy związane z powtarzaniem i przewidywalnością haseł.	Test teoretyczny
	Dobiera odpowiedni sposób zastosowania MFA.	Test teoretyczny
Dobiera techniczne i fizyczne środki ochrony informacji do rodzaju zagrożenia.	Wskazuje zastosowanie szyfrowania i maskowania danych;	Test teoretyczny
	Dobiera podstawowe zabezpieczenia do sytuacji związanej z korzystaniem z poczty elektronicznej lub sieci.	Test teoretyczny
Rozpoznaje phishing, socjotechnikę i zagrożenia wewnętrzne oraz identyfikuje symptomy incydentu bezpieczeństwa.	Wskazuje cechy wiadomości phishingowej.	Test teoretyczny
	Identyfikuje potencjalne zagrożenia wynikające z działań użytkowników wewnętrznych.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Stosuje podstawowe wymagania prawne dotyczące ochrony danych, cyberbezpieczeństwa i ochrony sygnalistów.	Przyporządkowuje RODO, UODO, KRI i KSC do właściwych obszarów.	Test teoretyczny
	Wskazuje podstawowe zasady ochrony poufności zgłoszenia sygnalisty.	Test teoretyczny
	Wskazuje podstawowe obowiązki pracownika i organizacji;	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

TAK

Pytanie 2. Czy dokument lub wyraźnie 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 wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Szkolenie adresowane jest do osób chcących zdobyć wiedzę, umiejętności oraz kompetencje społeczne z zakresu rozpoznawania cyberzagrożeń, stosowania zasad higieny cyfrowej oraz realizacji procedur ochrony danych i reagowania na incydenty w organizacji zgodnie z wymogami.

Na szkoleniu część teoretyczna zajmuje około 20-25% czasu szkolenia, część praktyczna to 75-80% czasu szkolenia.

Szkolenie prowadzone jest w grupie od 4 do 24 osób, a warunki organizacyjne są zawsze dostosowywane do liczby osób na szkoleniu. Podczas szkolenia odbywa się zarówno praca zbiorowa (np. mini-wykład), praca indywidualna (np. ćwiczenia indywidualne), jak i praca w grupach (od 2 do 6 osób) zależności od potrzeb.

Ostatnie 30 minut usługi przeznaczone jest na przeprowadzenie walidacji efektów uczenia się. Narzędzia walidacyjne (test wiedzy) przygotowuje wyznaczony Walidator, wskazany w Karcie Usługi.

Procedura przeprowadzenia walidacji:

1. Po zakończeniu części dydaktycznej prowadzonej przez Trenera Walidator dołącza do szkolenia realizowanego zdalnie w czasie rzeczywistym za pośrednictwem platformy ClickMeeting.

- 2. Walidator udostępnia uczestnikom elektroniczny test teoretyczny, nadzoruje jego samodzielne wypełnianie w czasie rzeczywistym, a następnie zbiera, sprawdza i ocenia testy.
- 3. Wynik testu stanowi podstawę do weryfikacji osiągnięcia zakładanych efektów uczenia się. Uczestnicy są informowani o uzyskanym wyniku.
- 4. Na podstawie wyników testu Walidator dokonuje oceny osiągnięcia efektów uczenia się i sporządza Protokół z przebiegu walidacji.

Opisana procedura gwarantuje rozdzielność funkcji Trenera i Walidatora. Osoba przeprowadzająca walidację nie prowadzi zajęć dydaktycznych ani nie uczestniczy w części szkoleniowej usługi realizowanej za pośrednictwem platformy ClickMeeting.

Przywitanie, prezentacja trenera oraz programu szkolenia, kontrakt z uczestnikami.

Moduł 1. Fundamenty i polityka bezpieczeństwa informacji. Wprowadzenie do InfoSec. Definiowanie bezpieczeństwa informacji, ochrona przed nieautoryzowanym dostępem i zakłóceniami.Triada PID oraz 5 filarów: Poufność, integralność, dostępność, autentyczność i niezaprzeczalność danych w cyklu życia informacji.Rola i tworzenie polityk bezpieczeństwa: Dlaczego jeden błąd pracownika zagraża całej firmie? Instrukcje postępowania i formalny wymiar procedur. Bezpieczne onboarding i offboarding: Zasada minimalnych uprawnień (Least Privilege), kontrola przeszłości i ciągły monitoring aktywności.

Metody pracy:wykład interaktywny, prezentacja multimedialna, praktyczne działanie.

Moduł 2. Praktyczne zabezpieczenia i technika pracy. Zarządzanie hasłami wg standardów NIST: Długość vs. złożoność (min. 16 znaków), unikanie powtórzeń i wzorców.Uwierzytelnianie wieloskładnikowe (MFA): Mechanizmy działania, aplikacje uwierzytelniające i ochrona przed przejęciem konta.Menedżery haseł w praktyce. Przewaga profesjonalnych menedżerów nad rozwiązaniami w przeglądarkach; zasady bezpiecznego udostępniania i przechowywania hasła głównego.Techniczne i fizyczne środki ochrony: Szyfrowanie, maskowanie danych, szyfrowana transmisja, bezpieczne korzystanie z sieci, antywirusy/UTM, obsługa poczty e-mail i ochrona pomieszczeń/serwerowni.

Metody pracy: wykład interaktywny, prezentacja multimedialna, praktyczne działanie.

Moduł 3. Zagrożenia, incydenty i rola pracownika. Identyfikacja zagrożeń. Metody rozpoznawania socjotechniki, phishingu oraz zagrożeń wewnętrznych (połączenie czynnika ludzkiego i technologicznego).Cykl zarządzania incydem (wg NIST):Przygotowanie, Wykrywanie i analiza, Ograniczenie skutków i usuwanie, Działania poincydentalne. Rola pracowników i Inspektorów (IBI/IOD). Audyty bezpieczeństwa, analiza ryzyka oraz odpowiedzialność personelu za realizację wytycznych.Zarządzanie dostawcami: Weryfikacja standardów bezpieczeństwa podmiotów zewnętrznych.

Metody pracy: wykład interaktywny, studium przypadku, ćwiczenia praktyczne.

Moduł 4. Ramy prawne, ochrona sygnalistów i odpowiedzialność. Przegląd kluczowych regulacji: RODO, polska ustawa o ochronie danych osobowych (UODO), Krajowe Ramy Interoperacyjności (KRI) oraz Krajowy System Cyberbezpieczeństwa (KSC).Sankcje i kary za naruszenia: kary pieniężne PUODO (do 20 mln EUR lub 4% obrotu), przepisy karne ustawy UODO (kara grzywny, ograniczenia lub pozbawienia wolności do lat 2 lub 3), kary porządkowe z Kodeksu Pracy (upomnienie, nagana). Ochrona sygnalistów (Dyrektywa2019/1937 i polska ustawa). Zachowanie poufności zgłoszenia, wymogi formalne, ochrona prawna zgłaszającego i odpowiedzialność za fałszywe zgłoszenia.

Metody pracy: warsztat, wykład interaktywny, prezentacja multimedialna, praktyczne działanie.

Podsumowanie szkolenia.

Walidacja

Harmonogram

Liczba pozycji harmonogramu: 9

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 9 Przywitanie ...	Zajęcia	Sylwester Cieśla	05-11-2026	08:00	08:30	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
2 z 9 Moduł 1.	Zajęcia	Sylwester Cieśla	05-11-2026	08:30	10:00	01:30
3 z 9 -	Przerwa	-	05-11-2026	10:00	10:15	00:15
4 z 9 Moduł 2.	Zajęcia	Sylwester Cieśla	05-11-2026	10:15	11:45	01:30
5 z 9 -	Przerwa	-	05-11-2026	11:45	12:00	00:15
6 z 9 Moduł 3.	Zajęcia	Sylwester Cieśla	05-11-2026	12:00	13:30	01:30
7 z 9 -	Przerwa	-	05-11-2026	13:30	14:00	00:30
8 z 9 Moduł 4.	Zajęcia	Sylwester Cieśla	05-11-2026	14:00	15:30	01:30
9 z 9 -	Walidacja	-	05-11-2026	15:30	16:00	00:30

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	08:00
w tym suma godzin zajęć	06:30
w tym suma godzin walidacji	00:30
w tym suma przerw	01:00
Suma godzin dydaktycznych bez przerw	09:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 200,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	2 200,00 PLN

Koszt osobogodziny brutto

275,00 PLN

Koszt osobogodziny netto

275,00 PLN

Liczba godzin usługi

Rodzaj godzin

Liczba godzin

Liczba godzin zegarowych usługi

08:00

Prowadzący

Liczba prowadzących: 1



1 z 1

Sylwester Cieśla

Właściciel Centrum Zabezpieczenia Informacji Sp. z o.o. Ekspert, doradca oraz praktyk z wieloletnim doświadczeniem w obszarze ochrony danych osobowych, bezpieczeństwa informacji oraz nowoczesnych technologii informatycznych. Specjalizuje się w dostarczaniu kompleksowych rozwiązań z zakresu cyberbezpieczeństwa i zarządzania ryzykiem dla sektora prywatnego oraz publicznego. Jako trener i konsultant prowadzi doradztwo indywidualne dla przedsiębiorstw i instytucji, a także realizuje audyty, wdrożenia technologii oraz optymalizację systemów teleinformatycznych. Kluczowe uprawnienia i kwalifikacje: Biegły Sądowy przy Sądzie Okręgowym w Kielcach w dziedzinie: Informatyka; Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji wg normy PN-EN ISO/IEC 27001; Pełnomocnik i Audytor Wewnętrzny Systemu Zarządzania Bezpieczeństwem Informacji wg ISO/IEC 27001. Certyfikowany Inspektor Ochrony Danych (IOD) / Administrator Bezpieczeństwa Informacji (ABI). Zainteresowania: komputery, muzyka, sport, samochody, programowanie.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnik szkolenia otrzyma autorskie materiały szkoleniowe (prezentacja multimedialna lub skrypt).

Warunki uczestnictwa

Osoba zainteresowana skorzystaniem z usługi rozwojowej z dofinansowaniem musi zarejestrować się w Bazie Usług Rozwojowych oraz dokonać zapisu na usługę przed jej rozpoczęciem, z użyciem numeru ID wsparcia.

Informacje dodatkowe

Czas trwania usługi szkoleniowej to 8 godzin zegarowych. Szkolenie jest jednodniowe, ujęte w 4 moduły. Planujemy przerwy pomiędzy modułami.

Usługa jest zwolniona z podatku VAT w przypadku, kiedy przedsiębiorstwo zwolnione jest z podatku VAT lub dofinansowanie wynosi co najmniej 70%. W innej sytuacji do ceny netto doliczany jest podatek VAT w wysokości 23%.

Podstawa: §3 ust. 1 pkt. 14 rozporządzenia Ministra Finansów z dnia 20.12.2013 r. w sprawie zwolnień od podatku od towarów i usług oraz szczegółowych warunków stosowania tych zwolnień (Dz. U. z 2018 r. poz. 701 z późn. zm.).

Warunki techniczne

Szkolenia odbywają się na platformie ClickMeeting w formie Webinaru.

Warunki techniczne niezbędne do udziału w usłudze:

Każdy komputer używany na co dzień będzie wystarczający do uczestnictwa w usłudze rozwojowej. Rekomendujemy udział w szkoleniu za pośrednictwem komputera. Tablet a zwłaszcza smartfon może być mniej praktyczny ze względu na wielkość ekranu.

1. Komputer/laptop – najlepiej, procesor Intel Core od i3 w górę, zalecane 4 GB RAM lub więcej, tablet 3 GB RAM lub smartfon.
2. Stałe łącze internetowe w dowolnej technologii – światłowod, GSM 3G lub 4G/LTE, Internet kablowy, zalecane min. 3 Mb/s w zakresie pobierania i wysyłania danych.
3. W miarę możliwości najnowszy system operacyjny: Windows 10 lub 8, 7, Vista z SP1; macOS X z macOS 10.7 lub nowszy, iOS 10 lub nowszy lub dedykowana aplikacja mobilna z AppStore lub GooglePlay, Android w wersji 4.0.4 lub nowszy w przypadku tabletów lub inne systemy operacyjne dające pewność odbioru transmisji bez zakłóceń.
4. Dowolna przeglądarka internetowa (zalecana Chrome lub Mozilla FireFox).
5. Głośniki lub słuchawki.

W trakcie szkolenia dostęp do wizji i dźwięku mają tylko trenerzy, uczestnicy szkolenia mogą komunikować się jedynie za pomocą czatu.

Link umożliwiający uczestnictwo w spotkaniu on-line ważny jest tylko w dniu szkolenia. Do każdego szkolenia przypisany jest oddzielny link.

Kontakt



Mirosław Kopik

E-mail mirek.kopik@eurodotacje.pl

Telefon (+48) 505 060 800