



## Kurs cyberbezpieczeństwa

Numer usługi 2024/01/25/30963/2057314

2 000,00 PLN brutto

2 000,00 PLN netto

125,00 PLN brutto/h

125,00 PLN netto/h

OŚRODEK  
SZKOLENIA  
DOKSZTAŁCANIA I  
DOSKONALENIA  
KADR KURSOR  
SPÓŁKA Z  
OGRANICZONĄ  
ODPOWIEDZIALNOŚ  
CIĄ



📍 zdalna w czasie rzeczywistym

🏠 Usługa szkoleniowa

🕒 16 h

📅 04.11.2024 do 05.11.2024

## Informacje podstawowe

<b>Kategoria</b>	Informatyka i telekomunikacja / Bezpieczeństwo IT
<b>Sposób dofinansowania</b>	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
<b>Grupa docelowa usługi</b>	Grupa docelowa kursu to kadra zarządzająca, specjaliści ds. bezpieczeństwa informacji i pracownicy odpowiedzialni za przetwarzanie danych. Adresowany jest do profesjonalistów z różnych branż, którzy chcą poszerzyć swoją wiedzę w obszarze cyberbezpieczeństwa, z naciskiem na ochronę danych osobowych. Odpowiedni dla firm, instytucji i organizacji, które pragną skutecznie zarządzać ryzykiem i spełniać obowiązujące normy prawne.
<b>Minimalna liczba uczestników</b>	5
<b>Maksymalna liczba uczestników</b>	30
<b>Data zakończenia rekrutacji</b>	28-10-2024
<b>Forma prowadzenia usługi</b>	zdalna w czasie rzeczywistym
<b>Liczba godzin usługi</b>	16
<b>Podstawa uzyskania wpisu do BUR</b>	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

# Cel

## Cel edukacyjny

podniesienie świadomości uczestników na temat zagrożeń związanych z zarządzaniem bezpieczeństwem informacji. Uczestnicy zdobędą praktyczne umiejętności zgodne z obowiązującymi przepisami oraz standardami ISO/IEC 27001, z naciskiem na ochronę danych osobowych. Szkolenie skupia się na identyfikacji, analizie i zarządzaniu ryzykiem, omawiając również najlepsze praktyki zabezpieczeń, nowe technologie oraz obowiązki związane z pracą zdalną.  
<https://www.kursor.edu.pl/szkolenia/oferta>

## Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnicy zdobędą umiejętności identyfikacji, analizy i minimalizacji zagrożeń, zwiększą świadomość obowiązków związanych z danymi osobowymi. Kurs obejmie również stosowanie nowych technologii w bezpieczeństwie, a uczestnicy zrozumieją konsekwencje prawne incydentów bezpieczeństwa informacji	Weryfikacja efektów uczenia obejmuje egzaminy, studia przypadków, projekty praktyczne, prezentacje, zadania domowe i ewaluacje symulacji. Ankiety zbierające opinie uczestników oceniają ich zrozumienie i satysfakcję z kursu, zapewniając kompleksową ocenę.	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

1) Obowiązki związane z przetwarzaniem danych i informacji prawnie chronionych:

- wymogi zachowania poufności w umowach z kontrahentami oraz powierzanie danych osobowych do przetwarzania z uwzględnieniem obowiązków podmiotu przetwarzającego na przykładach praktycznych,
- zasady i procedury udostępniania danych, w tym danych osobowych,

- c) odpowiedzialność związana z przetwarzaniem danych prawnie chronionych, o szczególnym znaczeniu strategicznym, w tym danych osobowych,
- d) wymogi prawne i obowiązki, a także dobre praktyki związane z wystąpieniem incydentu bezpieczeństwa informacji lub naruszenia danych osobowych oraz konsekwencje prawne dla kierownictwa w tym zakresie,
- 2) Identyfikacja, analiza i zarządzanie ryzykami w bezpieczeństwie informacji. Źródła i rodzaje zagrożeń związanych z bezpieczeństwem informacji oraz ich klasyfikacja w oparciu o możliwe zdarzenia i straty dla organizacji/instytucji,
- 3) Praktyczne podejście do analizy ryzyka i zarządzania ryzykiem w bezpieczeństwie informacji,
- 4) Najlepsze praktyki zabezpieczeń – na co należy zwracać uwagę przetwarzając informacje chronione metodą tradycyjną oraz za pomocą urządzeń takich jak komputer stacjonarny, laptop, smartphone, tablet, zewnętrzne nośniki danych, a także stosując nowe technologie itp.,
- 5) Bezpieczeństwo informacji, a nowe technologie: sztuczna inteligencja, biometria.
- 6) Odpowiedzialność oraz wskazówki dla użytkowników systemów teleinformatycznych w ramach codziennej pracy przy przetwarzaniu danych oraz z uwzględnieniem wykonywania pracy w formie zdalnej.
- 7) Omówienie zmian przepisów prawa pracy dotyczących pracy zdalnej i badania trzeźwości pracowników na przykładach praktycznych,
- 8) Warsztaty praktyczne – case study w trakcie szkolenia.

Certyfikat ukończenia kursu

Zaświadczenie wydane na podstawie § 23 ust. 4 rozporządzenia Ministra Edukacji i Nauki z dnia 6 października 2023 r. w sprawie kształcenia ustawicznego w formach pozaszkolnych (Dz. U. poz. 2175).

## 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 usługi brutto	2 000,00 PLN
Koszt usługi netto	2 000,00 PLN
Koszt godziny brutto	125,00 PLN
Koszt godziny netto	125,00 PLN

# Prowadzący

Liczba prowadzących: 0

Brak wyników.

## Informacje dodatkowe

### Informacje o materiałach dla uczestników usługi

skrypt tematyczny

### Informacje dodatkowe

Szkolenie może być realizowane zarówno raz jak i kilka razy w tygodniu w trybie dziennym, umożliwiając intensywną naukę i skoncentrowane zajęcia lub popołudniowym, co pozwala uczestnikom z innymi obowiązkami dostęp do wartościowej edukacji. Dodatkowo, istnieje opcja organizacji zajęć w formie weekendowej, co sprawia, że szkolenie staje się bardziej elastyczne i dostosowane do różnych harmonogramów życia. W związku z powyższym przedstawiony harmonogram może ulec zmianie - jesteśmy gotowi dostosować się do potrzeb całej grupy zapisanych osób, tworząc harmonogram, który uwzględni zróżnicowane preferencje czasowe uczestników.

## Warunki techniczne

platforma zoom

### Warunki techniczne szkolenia na platformie Zoom:

#### 1. Sprzęt komputerowy:

- Wymagany komputer PC lub Mac z dostępem do internetu.
- Zalecana kamera internetowa oraz mikrofon dla udziału w sesjach wideo.

#### 2. Przeglądarka internetowa:

- Zalecane przeglądarki: Google Chrome, Mozilla Firefox, Safari.
- Wymagane zaktualizowane wersje przeglądarek dla optymalnej wydajności.

#### 3. Stabilne połączenie internetowe:

- Minimalna prędkość łącza: 2 Mbps dla udziału w sesjach wideo.
- Zalecane połączenie kablowe dla stabilności.

#### 4. Platforma Zoom:

- Konieczne pobranie i zainstalowanie najnowszej wersji aplikacji Zoom przed szkoleniem.
- Aktywne konto Zoom (możliwość utworzenia bezpłatnego konta).

#### 5. System operacyjny:

- Kompatybilność z systemem Windows lub macOS.

#### 6. Oprogramowanie dodatkowe:

- Zalecane zainstalowanie najnowszych wersji programów, takich jak przeglądarka, Java, Flash itp.

#### 7. Dźwięk i słuchawki:

- Zalecane użycie słuchawek z mikrofonem dla lepszej jakości dźwięku.
- Sprawdzenie działania dźwięku przed rozpoczęciem szkolenia.

#### 8. Przygotowanie przed sesją:

- Testowanie sprzętu i połączenia przed planowanym szkoleniem.
- Zapewnienie cichego miejsca pracy dla minimalizacji zakłóceń.

#### 9. Wsparcie techniczne:

- Zapewnienie kontaktu z pomocą techniczną w razie problemów podczas sesji.

#### 10. Zaplanowane przerwy:

- Uwzględnienie krótkich przerw w grafiku dla odpoczynku uczestników.

Zapewnienie powyższych warunków technicznych umożliwi płynny przebieg szkolenia na platformie Zoom, zminimalizuje zakłócenia i zagwarantuje efektywną interakcję między prowadzącym a uczestnikami.

## Kontakt



**Jolanta Krzak**

**E-mail** [szkolenia.zamosc@kursor.edu.pl](mailto:szkolenia.zamosc@kursor.edu.pl)

**Telefon** (+48) 500 177 049