Możliwość dofinansowania

"Kurs cyberbezpieczeństwa"

Numer usługi 2024/06/20/30963/2191176

3 000,00 PLN brutto
3 000,00 PLN netto
187,50 PLN brutto/h
187,50 PLN netto/h

OŚRODEK SZKOLENIA DOKSZTAŁCANIA I DOSKONALENIA KADR KURSOR SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

★★★★★

zdalna w czasie rzeczywistym
Usługa szkoleniowa
16 h
09.12.2024 do 12.12.2024

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	• **Osoby początkujące** – osoby bez doświadczenia w cyberbezpieczeństwie, chcące zdobyć podstawową wiedzę o ochronie danych w sieci. • **Entuzjaści technologii** – osoby zainteresowane tematyką IT, które chcą zgłębić zagadnienia związane z bezpieczeństwem online. • **Studenci kierunków informatycznych** – osoby studiujące informatykę lub pokrewne kierunki, które chcą poszerzyć swoje kompetencje w zakresie zabezpieczeń systemów. • **Profesjonaliści IT** – specjaliści, którzy chcą poszerzyć swoje umiejętności o aktualne trendy i narzędzia z zakresu cyberbezpieczeństwa. • **Samoukowie** – osoby uczące się we własnym zakresie, które potrzebują ustrukturyzowanej wiedzy i praktycznych umiejętności.
Minimalna liczba uczestników	4
Maksymalna liczba uczestników	30
Data zakończenia rekrutacji	02-12-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	16

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

Usługa przygotowuje do samodzielnego pozyskiwania, zarządzania i sprawozdawczości w zakresie bezpieczeństwa informacji. Uczestnicy zdobędą umiejętności identyfikacji, analizy i minimalizacji zagrożeń, zgodnie z przepisami oraz standardami ISO/IEC 27001. Szkolenie obejmuje ochronę danych osobowych, najlepsze praktyki zabezpieczeń oraz stosowanie nowych technologii. Przygotowuje także do zarządzania ryzykiem i reagowania na incydenty bezpieczeństwa informacji w pracy zdalnej.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wiedza Efekt uczenia się: Uczestnik charakteryzuje zagrożenia związane z zarządzaniem bezpieczeństwem informacji i definiuje standardy ISO/IEC 27001.	Uczestnik wymienia główne rodzaje zagrożeń i ich źródła. Uczestnik opisuje podstawowe zasady i wymagania standardów ISO/IEC 27001. Uczestnik wyjaśnia konsekwencje prawne wynikające z naruszenia bezpieczeństwa informacji.	Test teoretyczny
Umiejętności Efekt uczenia się: Uczestnik projektuje procedury ochrony danych osobowych i monitoruje ich zgodność z obowiązującymi przepisami.	Uczestnik opracowuje plan zarządzania ryzykiem i procedury zabezpieczeń. Uczestnik wykonuje analizę ryzyka i identyfikuje słabe punkty w systemie zabezpieczeń. Uczestnik przeprowadza audyt zgodności z przepisami dotyczącymi ochrony danych osobowych.	Test teoretyczny
Kompetencje społeczne Efekt uczenia się: Uczestnik organizuje i nadzoruje zespół ds. bezpieczeństwa informacji, komunikując jasno zasady i procedury.	Uczestnik planuje i prowadzi spotkania zespołu, omawiając zadania i priorytety. Uczestnik ocenia efektywność działań zespołu i wprowadza niezbędne korekty. Uczestnik uzasadnia znaczenie przestrzegania procedur bezpieczeństwa w komunikacji z zespołem.	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

Interaktywna forma zdalna:

- Szkolenie odbywa się w formie zdalnej, w czasie rzeczywistym, za pomocą platformy Zoom. Umożliwia to uczestnictwo z dowolnego miejsca, oszczędzając czas i koszty związane z dojazdami. Interaktywne sesje wideo, współdzielenie ekranu i chat pozwalają na aktywny udział i bieżącą komunikację z prowadzącymi oraz innymi uczestnikami.

Godziny realizacji szkolenia:

- Szkolenie obejmuje 16 godzin edukacyjnych tj. 12 godzin zegarowych.
- Każda godzina szkolenia obejmuje 45 minut.

Przerwy:

- Przerwy nie są wliczone w czas trwania usługi.

Metody pracy:

- Zajęcia prowadzone są metodą ćwiczeniową, połączoną z rozmową na żywo oraz współdzieleniem ekranu. Warunkiem niezbędnym do osiągnięcia celu szkolenia jest samodzielne wykonanie wszystkich ćwiczeń zadanych przez trenera.

Harmonogram szkolenia:

- Szkolenie może być realizowane zarówno raz jaki 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 nie wskazano szczegółowego harmonogramu** - jesteśmy gotowi dostosować się do potrzeb całej grupy zapisanych osób, tworząc harmonogram, który uwzględni zróżnicowane preferencje czasowe uczestników.

Doświadczeni prowadzący:

- Zajęcia prowadzi ekspert z wieloletnim doświadczeniem w zakresie zarządzania bezpieczeństwem informacji. Uczestnicy mają możliwość czerpania z jego wiedzy i praktycznych wskazówek, co znacząco zwiększa efektywność nauki.

Certyfikat ukończenia:

- Po ukończeniu szkolenia uczestnicy otrzymują certyfikat potwierdzający nabycie kompetencji w zakresie cyberbezpieczeństwa. Certyfikat ukończenia kursu jest wydawany 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).

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

a) wymogi zachowania poufności w umowach z kontrahentami oraz powierzanie danych osobowych do przetwarzania z uwzględnieniem obowiązków podmiotu przetwarzającego na przykładach praktycznych,

b) 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 zarzadzanie 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.

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	3 000,00 PLN
Koszt usługi netto	3 000,00 PLN
Koszt godziny brutto	187,50 PLN
Koszt godziny netto	187,50 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 jaki 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

Anna Mirosław

E-mail szkolenia.lublin@kursor.edu.pl

Telefon (+48) 531 191 181