Możliwość dofinansowania

Cyberbezpieczeństwo i ochrona danych osobowych – szkolenie certyfikowane

Numer usługi 2025/10/16/10510/3082695

5 000,00 PLN brutto
5 000,00 PLN netto
263,16 PLN brutto/h
263,16 PLN netto/h

ZAKŁAD DOSKONALENIA ZAWODOWEGO W KATOWICACH

4,6 / 5

1 873 oceny

Żarki
Usługa szkoleniowa
stacjonarna
19:00 h
21.05.2026 do 18.06.2026

Informacje podstawowe

Kategoria	Prawo i administracja / Prawo pozostałe
Grupa docelowa usługi	**Kurs jest skierowany do:** • Specjalistów zajmujących się bezpieczeństwem systemów informatycznych i danych (m.in. specjalistów ds. cyberbezpieczeństwa) • Osób rozpoczynających karierę w obszarze cyberbezpieczeństwa lub planujących przebranżowienie • Inspektorów Ochrony Danych Osobowych oraz osób pełniących podobne funkcje • Osób zainteresowanych poszerzeniem wiedzy z zakresu cyberbezpieczeństwa i ochrony danych
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	5
Data zakończenia rekrutacji	07-05-2026
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	19
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 zdobycia kwalifikacji w zakresie stosowania zasad cyberbezpieczeństwa w praktyce zawodowej. Uczestnik zdobędzie wiedzę na temat podstawowych i zaawansowanych metod zabezpieczeń i ataków, pozna zasady funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji, aktualne zagrożenia w cyberprzestrzeni oraz aspekty ochrony danych osobowych w kontekście cyberzagrożeń.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje zasady ochrony informacji oraz bezpieczeństwa informacji.	omawia pojęcia: poufność, integralność, dostępność (CIA)	Test teoretyczny
	rozróżnia rodzaje zagrożeń (np. malware, phishing, ataki sieciowe)	Test teoretyczny
	wskazuje skutki naruszeń bezpieczeństwa	Test teoretyczny
Identyfikuje zagrożenia bezpieczeństwa oraz dobiera adekwatne metody ochrony.	rozpoznaje typowe ataki (np. phishing, ransomware)	Test teoretyczny
	wskazuje sposoby zapobiegania atakom	Test teoretyczny
	opisuje metody ograniczania ryzyka (np. aktualizacje, hasła, MFA)	Test teoretyczny
Stosuje podstawowe zasady ochrony danych osobowych zgodnie z przepisami prawa (RODO, UODO).	identyfikuje dane osobowe i szczególne kategorie danych	Test teoretyczny
	wskazuje podstawy przetwarzania danych	Test teoretyczny
	stosuje zasady minimalizacji i adekwatności danych	Test teoretyczny
Rozróżnia role i obowiązki w systemie ochrony danych osobowych.	opisuje zadania administratora danych, podmiotu przetwarzającego i IOD	Test teoretyczny
	wskazuje zakres odpowiedzialności poszczególnych ról	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Stosuje procedury związane z realizacją praw osób, których dane dotyczą oraz reagowaniem na naruszenia.	wymienia prawa osób (np. dostęp, sprostowanie, usunięcie danych)	Test teoretyczny
	opisuje procedurę zgłaszania naruszenia	Test teoretyczny
	wskazuje działania minimalizujące skutki incydentu	Test teoretyczny
Organizuje pracę własną zgodnie z zasadami bezpieczeństwa informacji i etyki zawodowej.	stosuje dobre praktyki bezpieczeństwa w codziennej pracy	Obserwacja w warunkach symulowanych
	przestrzega zasad poufności i odpowiedzialności	Obserwacja w warunkach symulowanych
Współpracuje w zespole w zakresie zapewnienia bezpieczeństwa informacji.	komunikuje zagrożenia w sposób zrozumiały dla zespołu	Obserwacja w warunkach symulowanych
	uczestniczy w rozwiązywaniu problemów bezpieczeństwa	Obserwacja w warunkach symulowanych
Przyjmuje odpowiedzialność za jakość wykonywanej pracy oraz rozwój kompetencji w obszarze bezpieczeństwa.	identyfikuje potrzeby rozwojowe	Obserwacja w warunkach symulowanych
	aktualizuje wiedzę w zakresie zagrożeń i przepisów	Obserwacja w warunkach symulowanych
	stosuje zasady odpowiedzialności zawodowej	Obserwacja w warunkach symulowanych

Kwalifikacje

Kwalifikacje niewłączone do ZSK

Uznane kwalifikacje

Pytanie 3. Czy dokument jest certyfikatem wydawanym przez międzynarodowe instytucje?

TAK

Strona internetowa Instytucji Certyfikującej: https://www.ecdl.ch/en/icdl/about-us/ecdl-foundation/

Strona internetowa Instytucji Walidującej: https://icdl.pl/

Informacje

Nazwa Podmiotu prowadzącego walidację	Walidację prowadzi Centrum Egzaminacyjne i Laboratorium Egzaminacyjne akredytowane przez Polskie Towarzystwo Informatyczne

Nazwa Podmiotu certyfikującego	ECDL Foundation

Program

I. Zrozumienie podstawowych zasad bezpieczeństwa i zagrożeń bezpieczeństwa (4 godziny, w tym 1 godzina zajęć praktycznych)

1. Co to jest informacja i dlaczego należy ją chronić?
2. Poufność; integralność; dostępność; wpływ zagrożenia i ryzyka;
3. Zasada najmniejszego przywileju; Inżynieria społeczna; analiza powierzchni ataku; modelowanie zagrożeń
4. **Zrozumienie bezpieczeństwa fizycznego**
   - Bezpieczeństwo obiektu;
   - Bezpieczeństwo komputera;
   - Wymienne urządzenia i dyski;
   - Kontrola dostępu;
   - Bezpieczeństwo urządzeń mobilnych;
   - Keyloggery
5. **Zrozumienie bezpieczeństwa w Internecie**
   - Ustawienia bezpieczeństwa przeglądarki;
   - Bezpieczne strony internetowe
6. **Szyfrowanie i podpisywanie poczty mail oraz inne zastosowania; wirtualna sieć prywatna (VPN);**
   - Klucz publiczny / klucz prywatny;
   - Algorytmy szyfrowania; właściwości certyfikatu;
   - Infrastruktura PKI / usługi certyfikacyjne;
   - Tokeny sprzętowe, ograniczenie urządzeń, aby uruchamiały tylko zaufane aplikacje
7. **Rodzaje ataków**
   - Phishing
   - Spoofing
   - Smishing
   - Vishing
   - Ataki przez pocztę elektroniczną
   - Deepfake
   - Kradzieże tożsamości
   - Ransomware
   - Malware
   - Kradzieże i wyłudzenia informacji
   - Ataki kierowane przez media społecznościowe
8. **Metody obrony i przeciwdziałania**
   - Zabezpieczenie sprzętu i nośników danych
   - Klucze sprzętowe
   - Zarządzanie hasłami i dostępem do danych
   - Weryfikacja dwuetapowa 2FA
   - Polityka haseł
   - Hasła – tworzenie bezpiecznych haseł
   - Menadżer haseł
   - Monitorowanie systemów i sieci
   - Procedury bezpieczeństwa i polityki organizacyjne
   - Szkolenia z zakresu bezpieczeństwa i edukacja pracowników
   - Ochrona danych w czasie ich przesyłania i przechowywania
   - Regularne aktualizacje i ochrona przed złośliwym oprogramowaniem
   - Tworzenie kopii zapasowych i odzyskiwanie danych
   - Segregacja danych i klasyfikacja informacji
   - Wdrożenie i przestrzeganie standardów ochrony poczty elektronicznej

II. Krajobraz cyberbezpieczeństwa (4 godzin w tym 1 godzina zajęć praktycznych)

1. **Stan cyberbezpieczeństwa w roku 2024**

- Raporty NIK
- Raporty CERT Polska
- Raporty CSIRT NASK

2. **Główne zagrożenia**
3. **Metody ataków**
4. **Jak się chronić?**
5. **Zarządzanie bezpieczeństwem informacji**
   - System Zarządzania Bezpieczeństwem informacji (SZBI)
   - Identyfikacja ryzyk związanych z prywatnością i ich konsekwencje prawne
   - Zasady szacowania ryzyka i ocena wpływu zastosowania określonych rozwiązań w zakresie
   - Skuteczności zarządzania bezpieczeństwem
   - Jak rozumieć i stosować podejście oparte na ryzyku – praktyczne wypełnienie szablonu Analizy Ryzyka
   - Zarządzanie cyklem życia danych osobowych
   - Omówienie wymagań normy ISO 27001
   - Wytyczne normy ISO 27002:2017 jako wykaz dobrych praktyk z zakresu bezpieczeństwa danych i informacji
   - Kontrola dostępu,
   - Kryptografia,
   - Bezpieczeństwo fizyczne,
   - Bezpieczna eksploatacja, w tym kopie zapasowe,
   - Bezpieczeństwo komunikacji,
   - Pozyskiwanie, rozwój i utrzymywanie systemów,
   - Zarządzanie incydentami bezpieczeństwa danych i informacji,
   - Zarządzanie ciągłością działania,
   - Zgodność z przepisami prawa.
   - Rola, zadania i uprawnienia Data Security Officer;
   - Auditowanie systemów bezpieczeństwa danych i informacji,
   - Cyberhigiena.

III. Podstawowe zasady przetwarzania danych osobowych (10 godzin, w tym 2 godziny zajęć praktycznych)

1. **Podstawy Ochrony**

- RODO - podstawowe informacje oraz definicje - wybrane zagadnienia
- Dane osobowe
- Przetwarzanie danych osobowych
- Podstawy prawne przetwarzania danych osobowych
- Obowiązki administratora
- Obowiązki Podmiotu przetwarzającego
- Prawa osób, których dane są przetwarzane
- Administracyjne kary pieniężne
- Obowiązki Inspektora Ochrony Danych Osobowych
- Postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych
- Odpowiedzialność cywilna, karna i administracyjna
- Przesłanki dopuszczalności przetwarzania danych osobowych (zwykłych i szczególnie chronionych)
- Ocena skutków dla ochrony danych
- Ochrona danych w fazie projektowania
- Domyślna ochrona danych
- Podstawy prawne przekazywania danych osobowych do państwa trzeciego
- Ochrona danych osobowych w stosunkach pracy
- Zasady przetwarzania danych osobowych na stanowiskach pracy

Czas trwania usługi: 19 godz. w tym 14 godzin zajęć teoretycznych, 4 godzin zajęć praktycznych oraz 1 godzina przeznaczona na walidację.

1 godzina zajęć = 45 min (godzina dydaktyczna).

Przerwy nie są wliczone w czas usługi rozwojowej.

Walidacja/Egzamin końcowy (1h)

Walidacja trwa łącznie **1 godzinę** i składa się z części teoretycznej oraz praktycznej.

Część teoretyczna realizowana jest w formie testu wiedzy. Weryfikowana jest znajomość zasad ochrony informacji, podstaw prawnych ochrony danych osobowych (RODO, UODO), obowiązków administratora i podmiotu przetwarzającego, procedur postępowania przy naruszeniu danych oraz kompetencji etycznych i organizacyjnych w pracy zawodowej.

Część praktyczna odbywa się poprzez obserwację w warunkach symulowanych. Uczestnik wykazuje umiejętność rozpoznawania typowych zagrożeń i ataków (w tym metod inżynierii społecznej), stosowania zasad ochrony danych i systemów w praktyce, współpracy w zespole oraz odpowiedzialnego wykonywania zadań, w tym podejmowania decyzji w sytuacjach problemowych.

Walidacja jest wliczona w czas trwania usługi rozwojowej. Po pozytywnym zaliczeniu walidacji uczestnik otrzymuje certyfikat ECDL/ICDL. Orientacyjny czas oczekiwania na wydanie certyfikatu wynosi od kilku dni do około 2–4 tygodni od momentu zatwierdzenia wyników egzaminu i przekazania ich do systemu certyfikacji ECDL/ICDL. Czas wydania certyfikatu może zależeć od procedur administracyjnych oraz formy wydawanego dokumentu.

Harmonogram

Liczba pozycji harmonogramu: 23

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 23 Zrozumienie podstawowych zasad bezpieczeństwa i zagrożeń bezpieczeństwa	Paweł Kiełkowicz	21-05-2026	15:00	15:45	00:45
2 z 23 Zrozumienie podstawowych zasad bezpieczeństwa i zagrożeń bezpieczeństwa	Paweł Kiełkowicz	21-05-2026	15:45	16:30	00:45
3 z 23 Przerwa	Paweł Kiełkowicz	21-05-2026	16:30	16:45	00:15
4 z 23 Zrozumienie podstawowych zasad bezpieczeństwa i zagrożeń bezpieczeństwa	Paweł Kiełkowicz	21-05-2026	16:45	17:30	00:45
5 z 23 Zrozumienie podstawowych zasad bezpieczeństwa i zagrożeń bezpieczeństwa	Paweł Kiełkowicz	21-05-2026	17:30	18:15	00:45
6 z 23 Krajobraz cyberbezpieczeństwa	Paweł Kiełkowicz	21-05-2026	18:15	19:00	00:45

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
7 z 23 Krajobraz cyberbezpieczeństwa	Paweł Kiełkowicz	22-05-2026	15:00	15:45	00:45
8 z 23 Krajobraz cyberbezpieczeństwa	Paweł Kiełkowicz	22-05-2026	15:45	16:30	00:45
9 z 23 Przerwa	Paweł Kiełkowicz	22-05-2026	16:30	16:45	00:15
10 z 23 Krajobraz cyberbezpieczeństwa	Paweł Kiełkowicz	22-05-2026	16:45	17:30	00:45
11 z 23 Podstawowe zasady przetwarzania danych osobowych	Paweł Kiełkowicz	22-05-2026	17:30	18:15	00:45
12 z 23 Podstawowe zasady przetwarzania danych osobowych	Paweł Kiełkowicz	22-05-2026	18:15	19:00	00:45
13 z 23 Podstawowe zasady przetwarzania danych osobowych	Paweł Kiełkowicz	25-05-2026	15:00	15:45	00:45
14 z 23 Podstawowe zasady przetwarzania danych osobowych	Paweł Kiełkowicz	25-05-2026	15:45	16:30	00:45
15 z 23 Przerwa	Paweł Kiełkowicz	25-05-2026	16:30	16:45	00:15
16 z 23 Podstawowe zasady przetwarzania danych osobowych	Paweł Kiełkowicz	25-05-2026	16:45	17:30	00:45

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
17 z 23 Podstawowe zasady przetwarzania danych osobowych	Paweł Kiełkowicz	25-05-2026	17:30	18:15	00:45
18 z 23 Podstawowe zasady przetwarzania danych osobowych	Paweł Kiełkowicz	25-05-2026	18:15	19:00	00:45
19 z 23 Podstawowe zasady przetwarzania danych osobowych	Paweł Kiełkowicz	26-05-2026	15:00	15:45	00:45
20 z 23 Podstawowe zasady przetwarzania danych osobowych	Paweł Kiełkowicz	26-05-2026	15:45	16:30	00:45
21 z 23 Przerwa	Paweł Kiełkowicz	26-05-2026	16:30	16:45	00:15
22 z 23 Podstawowe zasady przetwarzania danych osobowych	Paweł Kiełkowicz	26-05-2026	16:45	17:30	00:45
23 z 23 Walidacja	Paweł Kiełkowicz	27-05-2026	15:00	15:45	00:45

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 000,00 PLN
Koszt przypadający na 1 uczestnika netto	5 000,00 PLN

Koszt osobogodziny brutto	263,16 PLN
Koszt osobogodziny netto	263,16 PLN
W tym koszt walidacji brutto	50,00 PLN
W tym koszt walidacji netto	50,00 PLN
W tym koszt certyfikowania brutto	233,70 PLN
W tym koszt certyfikowania netto	233,70 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Paweł Kiełkowicz

Wykształcenie wyższe w zakresie socjologii – studia licencjackie na kierunku socjologia w zakresie komunikowania społecznego oraz studia magisterskie na kierunku socjologia ze specjalnością kierownictwo i przywództwo w społecznościach lokalnych, ukończone w Górnośląskiej Wyższej Szkole Handlowej im. Wojciecha Korfantego w Katowicach.

Posiada dodatkowe kwalifikacje zdobyte w ramach licznych kursów i szkoleń specjalistycznych z zakresu m.in. zarządzania zespołem, komunikacji interpersonalnej, technik marketingowych i sprzedażowych, ochrony danych osobowych (RODO), radzenia sobie w sytuacjach kryzysowych oraz przeciwdziałania i reagowania na zachowania agresywne, w tym technik behawioralnych i interwencyjnych.

W ciągu ostatnich 5 lat prowadził szkolenia jako wykładowca w obszarze cyberbezpieczeństwa, co potwierdza aktualne doświadczenie dydaktyczne powiązane z tematyką prowadzonych usług.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy szkolenia otrzymują komplet materiałów dydaktycznych, w tym:

- zeszyt,
- długopis,
- skrypt

Informacje dodatkowe

Usługa rozwojowa obejmuje łącznie **19 godzin dydaktycznych**, w tym:

- **14 godzin** zajęć teoretycznych,

- **4 godzin** zajęć praktycznych,
- **1 godzina** przeznaczona na **walidację**

Czas trwania jednej godziny dydaktycznej wynosi 45 minut.

Przerwy nie są wliczane do czasu trwania usługi rozwojowej.

Adres

ul. Sosnowa 2
42-310 Żarki
woj. śląskie

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Laboratorium komputerowe

Kontakt

Carmen Ceballos

E-mail c.ceballos@zdz.katowice.pl
Telefon (+48) 603 307 404