Możliwość dofinansowania

Cyberbezpieczeństwo i ochrona danych osobowych

Numer usługi 2026/04/21/10510/3501910

4 500,00 PLN brutto
4 500,00 PLN netto
225,00 PLN brutto/h
225,00 PLN netto/h
210,56 PLN cena rynkowa

ZAKŁAD DOSKONALENIA ZAWODOWEGO W KATOWICACH

4,6 / 5

1 877 ocen

Częstochowa
Usługa szkoleniowa
stacjonarna
20:00 h
29.06.2026 do 02.07.2026

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	08-06-2026
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	20
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
Wyjaśnia znaczenie ochrony informacji i podstawowe zasady bezpieczeństwa informacji.	Identyfikuje i opisuje różne rodzaje zagrożeń oraz ich wpływ na systemy informatyczne.	Test teoretyczny
Rozpoznaje typowe ataki oraz wskazuje sposoby obrony przed nimi.	Rozpoznaje metody inżynierii społecznej i opisuje sposoby ograniczania powierzchni ataku.	Obserwacja w warunkach symulowanych
Rozumie podstawy prawne ochrony danych osobowych (RODO, UODO).	Stosuje podstawowe zasady ochrony danych i systemów w środowisku pracy.	Test teoretyczny
Rozumie obowiązki administratora, podmiotu przetwarzającego i IOD.	Identyfikuje rodzaje danych osobowych i podstawy ich przetwarzania.	Test teoretyczny
Wyjaśnia prawa osób, których dane są przetwarzane.	Stosuje procedury postępowania w przypadku naruszenia danych.	Test teoretyczny
		Obserwacja w warunkach symulowanych
Wykazuje się wysoko rozwiniętymi kompetencjami społecznymi na swoim stanowisku pracy.	Organizuje własną pracę w zgodzie z zasadami etyki zawodowej.	Test teoretyczny
	Współpracuje w zespole zadaniowym.	Obserwacja w warunkach symulowanych
	Przyjmuje odpowiedzialność za jakość pracy i rozwój zawodowy.	Obserwacja w warunkach symulowanych

Kwalifikacje

Kwalifikacje niewłączone do ZSK

Uznane kwalifikacje

Pytanie 1. Czy dokument jest wydany przez podmiot systemu oświaty lub szkolnictwa wyższego na podstawie odrębnych przepisów?

TAK

rozporządzenie Ministra Edukacji i Nauki z dnia 6 października 2023 r. w sprawie kształcenia ustawicznego w formach pozaszkolnych (Dz. U. poz. 2175 oraz z 2024 r. poz. 1854)

Informacje

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

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

Harmonogram

Liczba pozycji harmonogramu: 0

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	4 500,00 PLN
Koszt przypadający na 1 uczestnika netto	4 500,00 PLN
Koszt osobogodziny brutto	225,00 PLN
Koszt osobogodziny netto	225,00 PLN
W tym koszt walidacji brutto	250,00 PLN
W tym koszt walidacji netto	250,00 PLN
W tym koszt certyfikowania brutto	250,00 PLN
W tym koszt certyfikowania netto	250,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Piotr Dobosz

Pan Piotr Dobosz jest absolwentem Politechniki Częstochowskiej, gdzie ukończył studia magisterskie na kierunkach Informatyka o specjalnościach: Inżynieria oprogramowania i systemy informatyczne oraz Sieci komputerowe. Posiada tytuł magistra inżyniera informatyki.
W trakcie kariery zawodowej stale podnosił kwalifikacje, uzyskując liczne certyfikaty branżowe: Microsoft Technology Associate (MTA) – cztery certyfikaty z obszaru infrastruktury IT oraz dwa z

zakresu programowania (Certiport, 2013),
Instruktor Akademii CISCO – uprawnienia do uruchamiania i prowadzenia kursów Akademii CISCO (2018),
Certyfikat IT Essentials umożliwiający prowadzenie szkoleń z zakresu podstaw informatyki i sprzętu komputerowego (2018),
C++ Programming Associate – potwierdzający znajomość języka programowania C++ (CISCO Academy / C++ Institute Partner, 2018),
Google Scholarship – Android Advanced Programming – ukończony kurs zaawansowanego programowania aplikacji na system Android w ramach stypendium Google (2017–2018).

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 **20 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. Jagiellońska 141
42-202 Częstochowa
woj. śląskie

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Laboratorium komputerowe

Kontakt

Ewelina Pawłowska

E-mail czestochowa@zdz.katowice.pl
Telefon (+48) 697 818 686