Możliwość dofinansowania

Bezpieczny Internet i Komputer – Kurs ICDL z egzaminem IT SECURITY dla Dorosłych

Numer usługi 2026/06/30/192140/3658496

4 950,00 PLN brutto
4 950,00 PLN netto
253,85 PLN brutto/h
253,85 PLN netto/h
261,33 PLN cena rynkowa

Centrum Szkoleniowo - Rekrutacyjne SILESIA Bogumiła Kłosowska

4,8 / 5

273 oceny

Szczyrk
Usługa szkoleniowa
stacjonarna
Zajęcia grupowe
19:30 h
10.07.2026 do 12.07.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Kurs przeznaczony jest dla osób dorosłych, w szczególności pracowników biurowych oraz seniorów, którzy chcą bezpiecznie i świadomie korzystać z komputera oraz Internetu w pracy i w życiu codziennym. Skierowany jest do osób na poziomie podstawowym i średnim, bez specjalistycznej wiedzy IT, które chcą nauczyć się chronić swoje dane, rozpoznawać zagrożenia (np. oszustwa internetowe) oraz zwiększyć swoje kompetencje cyfrowe.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	03-07-2026
Forma prowadzenia usługi	stacjonarna
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 bezpiecznego i świadomego korzystania z komputera oraz Internetu, w tym rozpoznawania zagrożeń, ochrony danych osobowych i stosowania podstawowych zasad cyberbezpieczeństwa, a także przygotowuje do zdania egzaminu ICDL IT Security.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
definiuje podstawowe pojęcia związane z bezpieczeństwem IT oraz identyfikuje zagrożenia dla danych	• definiuje pojęcia: dane, informacja, cyberprzestępczość	Test teoretyczny
	• rozpoznaje przykłady zagrożeń dla danych w życiu codziennym	Test teoretyczny
rozpoznaje zagrożenia związane z socjotechniką i kradzieżą tożsamości.	• wskazuje znaczenie ochrony danych osobowych	Test teoretyczny
	• identyfikuje przykłady phishingu i innych metod socjotechniki	Test teoretyczny
	• wskazuje konsekwencje kradzieży tożsamości	Test teoretyczny
	• opisuje sposoby unikania zagrożeń	Analiza dowodów i deklaracji
stosuje podstawowe metody zabezpieczania danych i plików	• tworzy bezpieczne hasła zgodne z zasadami	Test teoretyczny
	• zabezpiecza pliki hasłem lub szyfrowaniem	Analiza dowodów i deklaracji
	• rozróżnia bezpieczne i niebezpieczne sposoby przechowywania danych	Test teoretyczny
identyfikuje zagrożenia związane ze złośliwym oprogramowaniem i stosuje metody ochrony.	• rozpoznaje typy złośliwego oprogramowania	Test teoretyczny
	• wykonuje skanowanie antywirusowe	Test teoretyczny
	• wskazuje znaczenie aktualizacji oprogramowania	Test teoretyczny
bezpiecznie korzysta z sieci komputerowych i Internetu.	• rozróżnia typy sieci i ich zastosowanie	Test teoretyczny
	• wskazuje zagrożenia związane z sieciami Wi-Fi	Analiza dowodów i deklaracji
	• stosuje podstawowe zasady bezpiecznego połączenia z siecią	Analiza dowodów i deklaracji
zarządza dostępem do systemów i stosuje zasady bezpiecznego logowania.	• stosuje zasady tworzenia i zarządzania hasłami	Analiza dowodów i deklaracji
	• rozpoznaje metody uwierzytelniania (np. MFA)	Analiza dowodów i deklaracji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
bezpiecznie korzysta z usług internetowych i komunikacji elektronicznej.	• rozpoznaje bezpieczne strony internetowe	Analiza dowodów i deklaracji
	• identyfikuje podejrzane wiadomości e-mail	Test teoretyczny
	• stosuje zasady bezpieczeństwa w mediach społecznościowych	Test teoretyczny
wykonuje kopie zapasowe oraz bezpiecznie zarządza danymi.	• tworzy kopię zapasową danych	Analiza dowodów i deklaracji
	• przywraca dane z kopii zapasowej	Analiza dowodów i deklaracji
wykazuje odpowiedzialność za bezpieczeństwo danych własnych i powierzonych	• uświadamia odbiorcom zagrożenia cyfrowe i reaguje na nie w sposób odpowiedzialny	Analiza dowodów i deklaracji
	• dba o ochronę prywatności swojej i innych użytkowników	Analiza dowodów i deklaracji
	• motywuje do przestrzegania zasad etycznych i prawnych związanych z korzystaniem z technologii IT	Analiza dowodów i deklaracji

Kwalifikacje

Kwalifikacje niewłączone do ZSK

Uznane kwalifikacje

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

TAK

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

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

Informacje

Nazwa Podmiotu prowadzącego walidację	Laboratorium Egzaminacyjne akredytowane przez PTI jest w BUR
Nazwa Podmiotu certyfikującego	Polskie Towarzystwo Informatyczne (nie jest w BUR)

Program

Program szkolenia:

1.Wprowadzenie do bezpieczeństwa IT

Podstawowe pojęcia: dane i informacje, zagrożenia dla danych, cyberprzestępczość, znaczenie ochrony danych osobowych i prywatności.

2.Zagrożenia i bezpieczeństwo osobiste

Oszustwa internetowe: socjotechnika, phishing, kradzież tożsamości.

Sposoby rozpoznawania i unikania zagrożeń w codziennym użytkowaniu. Przykłady działań oszustów

3.Bezpieczeństwo plików i danych

Bezpieczne hasła, szyfrowanie danych, ochrona dokumentów oraz zasady bezpiecznego przechowywania informacji.

Metody uwierzytelniania, uwierzytelnianie wieloskładnikowe oraz zarządzanie dostępem do kont.

4.Złośliwe oprogramowanie (malware)

Rodzaje zagrożeń (wirusy, trojany, robaki), sposoby infekcji oraz metody ochrony i usuwania zagrożeń.

5.Ochrona komputera. Bezpieczeństwo sieci i połączeń

Programy antywirusowe, aktualizacje systemu i aplikacji, skanowanie oraz dobre praktyki bezpieczeństwa. Przykłady aplikacji antywirusowych.

Typy sieci (LAN, Wi-Fi, VPN), zagrożenia sieciowe, zapora sieciowa (firewall) oraz bezpieczne korzystanie z sieci bezprzewodowych.

6.Bezpieczne korzystanie z Internetu i przeglądarek

Ustawienia przeglądarki, bezpieczne strony internetowe, zakupy online, rozpoznawanie fałszywych witryn.

Dobre praktyki w pracy z komputerem, Internetem, urządzeniami mobilnymi. Jak działają i jak zabezpieczać narzędzia Internetu Rzeczy

7.Bezpieczna komunikacja i urządzenia mobilne

Bezpieczeństwo e-maili, rozpoznawanie phishingu, sieci społecznościowe, komunikatory oraz zagrożenia mobilne.

Sposoby reagowania i zabezpieczania się przed zagrożeniami podczas korzystania z komputera, telefonu, sieci internetowej. Przedstawienie narzędzi do ochrony

8.Kopie zapasowe i zarządzanie danymi

Tworzenie i przywracanie kopii zapasowych, bezpieczne usuwanie danych

Narzędzia diagnostyczne służące do poprawy działania komputera i telefonu.

Informacja o egzaminie

Po zakończeniu szkolenia uczestnicy przystępują do egzaminu certyfikującego IT SECURITY (S3) który potwierdza znajomość głównych zasad związanych z zabezpieczeniem informacji i danych, fizycznym bezpieczeństwem, prywatnością i postępowaniem w przypadku kradzieży tożsamości, który jest organizowany i oceniany przez podmiot zewnętrzny. Certyfikat potwierdzający nabycie kwalifikacji zostaje wydany uczestnikowi w dniu egzaminu.

Zgodnie z Załącznikiem nr 2 do „Wytycznych w zakresie monitorowania postępu rzeczowego realizacji programów operacyjnych na lata2021-2027” certyfikat ICDL (ECDL) jest kwalifikacją, a Polskie Towarzystwo Informatyczne – instytucją certyfikującą dla tej kwalifikacji.

Rozliczenie godzin szkolenia:

Liczba godzin szkolenia to 19:30 h (z czego 12h praktycznych, 5:30 h teoretycznych, 2h egzamin)

W harmonogramie uwzględniono przerwy w usłudze i są one wliczone w czas usługi rozwojowej.

Egzamin jest wliczony w czas usługi rozwojowej. 19:30 godzin zegarowych wynika z wyliczenia systemu BUR.

Warunki organizacyjne:

Warunki organizacyjne dla przeprowadzenia usługi: każdy z uczestników szkolenia będzie miał dostęp do komputera z systemem operacyjnym Windows, oprogramowaniem niezbędnym do przeprowadzenia usługi oraz podłączeniem do Internetu

---

Harmonogram

Liczba pozycji harmonogramu: 13

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 13 Wprowadzenie do bezpieczeństwa IT	Zajęcia	KRZYSZTOF SZLĘZAK	10-07-2026	14:45	17:00	02:15
2 z 13 -	Przerwa	-	10-07-2026	17:00	17:30	00:30
3 z 13 Zagrożenia i bezpieczeństwo osobiste	Zajęcia	KRZYSZTOF SZLĘZAK	10-07-2026	17:30	19:30	02:00
4 z 13 Bezpieczeństwo plików i danych	Zajęcia	KRZYSZTOF SZLĘZAK	11-07-2026	09:00	11:00	02:00
5 z 13 -	Przerwa	-	11-07-2026	11:00	11:15	00:15
6 z 13 Złośliwe oprogramowanie (malware)	Zajęcia	KRZYSZTOF SZLĘZAK	11-07-2026	11:15	13:15	02:00
7 z 13 -	Przerwa	-	11-07-2026	13:15	14:00	00:45
8 z 13 Ochrona komputera. Bezpieczeństwo sieci i połączeń	Zajęcia	KRZYSZTOF SZLĘZAK	11-07-2026	14:00	16:45	02:45

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
9 z 13 Ochrona komputera. Bezpieczeństwo sieci i połączeń	Zajęcia	KRZYSZTOF SZLĘZAK	12-07-2026	09:00	11:30	02:30
10 z 13 -	Przerwa	-	12-07-2026	11:30	12:00	00:30
11 z 13 Kopie zapasowe i zarządzanie danymi	Zajęcia	KRZYSZTOF SZLĘZAK	12-07-2026	12:00	14:00	02:00
12 z 13 -	Przerwa	-	12-07-2026	14:00	14:30	00:30
13 z 13 -	Walidacja	-	12-07-2026	14:30	16:00	01:30

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	19:30
w tym suma godzin zajęć	15:30
w tym suma godzin walidacji	01:30
w tym suma przerw	02:30
Suma godzin dydaktycznych bez przerw	22:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 950,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	4 950,00 PLN
Koszt osobogodziny brutto	253,85 PLN

Koszt osobogodziny netto	253,85 PLN
W tym koszt walidacji brutto	378,23 PLN
W tym koszt walidacji netto	378,23 PLN
W tym koszt certyfikowania brutto	378,23 PLN
W tym koszt certyfikowania netto	378,23 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	19:30

Prowadzący

Liczba prowadzących: 1

1 z 1

KRZYSZTOF SZLĘZAK

Trener z ponad 20-letnim doświadczeniem w branży IT, specjalizujący się w prowadzeniu szkoleń technicznych z zakresu systemów klasy CRM, technologii informatycznych, cyberbezpieczeństwa, Sztucznej Inteligencji (AI) oraz szerokiego wachlarza szkoleń z zakresu kompetencji cyfrowych, w tym ECCC i ECDL. Od lat przygotowuje uczestników szkoleń do egzaminów IEES, ECDL oraz ZRK. Członek stowarzyszenie Lepsza Polska (które ukierunkowuje swoje działania na rzecz ekologii oraz zrównoważonego rozwojowi). W ciągu ostatnich 5 lat koncentruje swoje działania na pogłębianiu wiedzy o zielonej gospodarce, zrównoważonym rozwoju i profilaktyce zdrowia cyfrowego, poprzez organizację i realizację szkoleń w tych obszarach. Współprowadził szkolenia związane z zrównoważonym rozwojem oraz raportowaniem zgodnym z normami CSRD. Jego zaangażowanie w rozwój zawodowy znajduje odzwierciedlenie w uczestnictwie w licznych kursach i szkoleniach, które pozwalają mu na bieżąco aktualizować i poszerzać wiedzę w zakresie nowych technologii, cyberbezpieczeństwa, umiejętności miękkich oraz ekologii. Jest wysoko ceniony za profesjonalizm, indywidualne podejście do uczestników oraz umiejętność przekazywania skomplikowanej wiedzy w sposób przystępny. Jego celem jest nie tylko rozwój kompetencji uczestników szkoleń, ale także szerzenie idei zrównoważonego rozwoju w kontekście nowoczesnych technologii i gospodarki.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Informacja o materiałach szkoleniowych.

Uczestnik szkolenia otrzymuje materiały szkoleniowe w postaci cyfrowej. Materiały mają postać skryptu z zakresu wiedzy omawianej na zajęciach oraz zestawu przykładowych ćwiczeń przygotowujących do egzaminu. Dystrybucja materiałów odbywa się drogą mailową na początku zajęć.

Adres

ul. Poziomkowa 20

43-370 Szczyrk

woj. śląskie

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi

Kontakt

BOGUMIŁA KŁOSOWSKA

E-mail bogumila.klosowska@csrsilesia.pl

Telefon (+48) 666 608 284