Możliwość dofinansowania

Cyberbezpieczeństwo w zrównoważonej transformacji cyfrowej - ochrona przed zagrożeniami dla początkujących użytkowników. Kwalifikacje. Szkolenie.

Numer usługi 2026/04/23/163842/3507728

6 081,12 PLN brutto
4 944,00 PLN netto
380,07 PLN brutto/h
309,00 PLN netto/h
175,00 PLN cena rynkowa

Digital Marketing
Krzysztof Szymak

★★★★★ 4,9 / 5

484 oceny

Rybnik / stacjonarna
Usługa szkoleniowa
16 h
30.06.2026 do 06.07.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Internet
Grupa docelowa usługi	Szkolenie skierowane jest do osób (w szczególności w wieku 55+), które planują z własnej inicjatywy podnieść swoje umiejętności w zakresie kwalifikacji cyfrowych - zarówno w obszarze podstawowej obsługi komputera, jak i cyberbezpieczeństwa. Usługa prowadzi do zdobycia kwalifikacji międzynarodowej **GCCS-DIG-004 Specjalista ds. cyberbezpieczeństwa**. Usługa szkoleniowa dedykowana jest także dla osób chcących podnieść swoje zielone kompetencje w zakresie bezpiecznego i zrównoważonego wykorzystywania technologii cyfrowych - od świadomego zarządzania danymi i ograniczania ich nadmiaru, przez energooszczędne korzystanie ze sprzętu i usług online, po odpowiedzialne i etyczne podejście do ochrony informacji i prywatności.
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	29-06-2026
Forma prowadzenia usługi	stacjonarna
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 szkoleniowa przygotowuje do samodzielnego, praktycznego zarządzania cyberbezpieczeństwem, z uwzględnieniem zasad zrównoważonego rozwoju. Uczestnicy nauczą się identyfikować i neutralizować zagrożenia, wdrażać zabezpieczenia oraz zarządzać danymi i infrastrukturą IT. Szkolenie rozwija umiejętności w obszarze technologii informacyjno-komunikacyjnych (ICT) oraz zielonych kompetencji, rozumianych jako bezpieczne, odpowiedzialne i efektywne korzystanie z zasobów cyfrowych.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozróżnia rodzaje zagrożeń cyberbezpieczeństwa oraz metody ich identyfikacji w systemach IT.	Wymienia co najmniej 5 rodzajów zagrożeń cyberbezpieczeństwa i ich charakterystyki.	Test teoretyczny
	Opisuje metody detekcji zagrożeń w infrastrukturze sieciowej.	Test teoretyczny
Wyjaśnia zasady energooszczędnego projektowania infrastruktury bezpieczeństwa IT i jej wpływ na środowisko.	Charakteryzuje wpływ serwerów i urządzeń sieciowych na zużycie energii i emisję CO2.	Test teoretyczny
	Opisuje technologie optymalizacji energetycznej w systemach bezpieczeństwa.	Test teoretyczny
Charakteryzuje przepisy prawne i normalizacyjne dotyczące ochrony danych i bezpieczeństwa informacji.	Wymienia obowiązujące regulacje prawne w zakresie ochrony danych osobowych.	Test teoretyczny
	Opisuje standardy i certyfikacje bezpieczeństwa informacyjnego.	Test teoretyczny
Wyjaśnia zasady zarządzania cyklem życia oprogramowania z uwzględnieniem zrównoważonego rozwoju.	Opisuje etapy cyklu życia oprogramowania i ich wpływ na produkcję e-odpadów.	Test teoretyczny
	Charakteryzuje znaczenie open-source i długoterminowego wsparcia dla zmniejszenia odpadów.	Test teoretyczny
Wdraża systemy monitorowania ruchu sieciowego z optymalizacją zużycia zasobów i energii.	Dobiera rozwiązania monitorujące minimalizujące obciążenie infrastruktury i zużycie energii.	Analiza dowodów i deklaracji
	Konfiguruje kompresję danych i archiwizację logów bezpieczeństwa.	Analiza dowodów i deklaracji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Obsługuje i zarządza sprzętem sieciowym zgodnie z zasadami gospodarki o obiegu zamkniętym.	Organizuje recykling elektroniczny i bezpieczne usuwanie danych ze sprzętu.	Analiza dowodów i deklaracji
	Planuje podejście do wycofywania starych urządzeń sieciowych.	Analiza dowodów i deklaracji
Projektuje i realizuje szkolenia pracowników dotyczące bezpieczeństwa danych z wykorzystaniem platform cyfrowych.	Wybiera platformy e-learningowe minimalizujące emisję CO2 i zużycie papieru.	Analiza dowodów i deklaracji
	Opracowuje materiały szkoleniowe w formacie cyfrowym dla efektywnego przekazu.	Analiza dowodów i deklaracji
Analizuje i redukuje ślad węglowy infrastruktury bezpieczeństwa IT poprzez optymalizację zasobów.	Identyfikuje sposoby redukcji zużycia energii w systemach monitorowania i ochrony.	Analiza dowodów i deklaracji
	Planuje migrację do modeli hybrydowych zasilanych energią odnawialną.	Analiza dowodów i deklaracji
Komunikuje zasady bezpieczeństwa danych pracownikom w sposób jasny, zrozumiały i konstruktywny.	Wyjaśnia złożone zagadnienia cyberbezpieczeństwa w prosty i przystępny sposób.	Test teoretyczny
	Adaptuje komunikację do różnych poziomów technicznych odbiorców.	Test teoretyczny
Odpowiedzialnie zarządza projektami bezpieczeństwa IT z uwzględnieniem wpływu na środowisko naturalne.	Podejmuje decyzje balansujące bezpieczeństwo danych z ochroną środowiska.	Test teoretyczny
	Dokumentuje i uzasadnia działania zmniejszające negatywny wpływ na ekologię.	Test teoretyczny
Współpracuje w zespole wielodyscyplinarnym w celu implementacji rozwiązań cyberbezpieczeństwa.	Koordynuje działania z pracownikami IT, menedżerami i specjalistami z innych dziedzin.	Test teoretyczny
	Zgłasza problemy i zagrożenia w sposób konstruktywny, proponując rozwiązania.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wykazuje zaangażowanie w ciągłe uczenie się i doskonalenie umiejętności w dynamicznym środowisku cyberzagrożeń.	Identyfikuje nowe trendy zagrożeń i metody zrównoważonego bezpieczeństwa.	Test teoretyczny
	Uczestniczy w szkoleniach podnoszących kompetencje zawodowe i świadomość ekologiczną.	Test teoretyczny

Kwalifikacje

Kwalifikacje niewłączone do ZSK

Uznane kwalifikacje

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

TAK

Strona internetowa Instytucji Certyfikującej: https://standardgccs.com/qualifications/

Strona internetowa Instytucji Walidującej: https://icvc.eu/kwalifikacje-miedzynarodowe/

Informacje

Nazwa Podmiotu prowadzącego walidację	ICVC CERTYFIKACJA SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ
Nazwa Podmiotu certyfikującego	TALENT ODYSSEY LTD.

Program

Efekty uczenia się, kryteria weryfikacji i metody walidacji są zależne od specyfikacji kwalifikacji międzynarodowej i nie podlegają ingerencji ze strony Dostawcy Usługi.

Usługa prowadzi do nabycia kwalifikacji: międzynarodowej **Specjalista ds. cyberbezpieczeństwa (GCCS-DIG-004).** W ramach szkolenia zapewniono **walidację efektów uczenia się**, mającą na celu ocenę poziomu osiągnięcia efektów kształcenia. Uczestnik, który pozytywnie ukończy proces walidacji i zda formalny egzamin, uzyskuje **kwalifikację międzynarodową: GCCS-DIG-004 Specjalista ds. cyberbezpieczeństwa.**

Szkolenie wpisuje się w cele **Regionalnej Strategii Innowacji Województwa Śląskiego 2030 (RIS WSL 2030)**, w szczególności w obszarach:

- **Technologie informacyjno-komunikacyjne (ICT),**
- **Zielona gospodarka.**

Program wspiera rozwój kompetencji w zakresie cyberbezpieczeństwa, ochrony danych oraz zrównoważonego zarządzania infrastrukturą IT, uwzględniając aspekty **efektywności energetycznej i ograniczania wpływu technologii cyfrowych na środowisko**.

Szkolenie odpowiada również na potrzeby transformacji regionu w kierunku gospodarki niskoemisyjnej i opartej na wiedzy, przygotowując uczestników do pracy w środowisku, w którym rośnie znaczenie bezpieczeństwa cyfrowego oraz odpowiedzialnego wykorzystania zasobów technologicznych.

Program odnosi się do **Programu Rozwoju Technologii Województwa Śląskiego** poprzez:

- rozwój kompetencji w zakresie cyberbezpieczeństwa i ochrony danych,
- praktyczne zastosowanie narzędzi i procedur bezpieczeństwa IT,
- kształtowanie umiejętności optymalizacji infrastruktury cyfrowej pod kątem energooszczędności.

Ukończenie szkolenia zwiększa konkurencyjność uczestników na rynku pracy oraz ich gotowość do pracy w sektorach związanych z cyberbezpieczeństwem, IT oraz zieloną transformacją.

Przykładowe perspektywy zawodowe:

- specjalista ds. cyberbezpieczeństwa w MŚP,
- koordynator bezpieczeństwa informacji,
- specjalista ds. ochrony danych i RODO,
- specjalista ds. green IT,
- konsultant ds. bezpieczeństwa cyfrowego.

Szkolenie będzie miało formę głównie warsztatową. Każdy uczestnik będzie pracował przy komputerze. **Forma warsztatowa zapewni realizację celu edukacyjnego usługi.**

Usługa realizowana jest w godzinach zegarowych, tj. 1 godzina lekcyjna = 60 minut.

Uwaga do harmonogramu: przerwy na lunch są wliczone w czas trwania usługi i zostały ustalone na godzinę 13:00-13:15 - uwzględniono w harmonogramie.

!!! WAŻNE: Szkolenie realizowane jest w terminie 30.06 - 06.07.2026 r. Po zakończeniu szkolenia uczestnicy przystępują do egzaminu certyfikującego, który jest organizowany i oceniany przez międzynarodowy podmiot zewnętrzny. Czas oczekiwania na wynik walidacji wynosi średnio ok. 5 dni roboczych od dnia przeprowadzenia egzaminu. W związku z tym - według Zał. 2 (2.4) do Regulaminu BUR **termin realizacji usługi został określony w karcie na 30.06 - 06.07.2026, ponieważ obejmuje:**

- **okres prowadzenia szkolenia (30 czerwca - 1 lipca)**
- **oraz okres oczekiwania na wynik walidacji (do 6 lipca).**

Część teoretyczna obejmuje 3,5 godziny zegarowe zajęć, natomiast część praktyczna - 9,5 godziny. Pozostały czas trwania usługi to: 2 przerwy (w pierwszym oraz drugim dniu zajęć) po 45 minut oraz 1,5 godziny przeznaczone na kwestie organizacyjne (m.in. przywitanie, pre-testy, post-testy, pytania, podsumowanie zajęć) i walidację usługi oraz egzamin.

PROGRAM:

I DZIEŃ SZKOLENIA [część teoretyczna: 2 godziny, część praktyczna: 5 godzin, przerwa: 45 min, kwestie organizacyjne: 15 min] - 30.06.2026:

08:30 - 08:45 Przywitanie uczestników, omówienie szkolenia, przeprowadzenie pre-testów w celu oceny początkowego poziomu wiedzy uczestników.

08:45 - 10:00 MODUŁ I: Anatomia komputera. Wprowadzenie do cyberbezpieczeństwa i eko-IT.

1. Sprzęt oraz oprogramowanie - co sprawia, że komputer działa (CPU, RAM, dysk – analogia do smartfona).
2. Wpływ podzespołów i serwerów na zużycie energii oraz emisję CO_2.
3. System operacyjny jako centrum zarządzania - personalizacja i bezpieczeństwo.
4. Zarządzanie oknami i skróty klawiszowe w pracy efektywnej energetycznie.
5. Wprowadzenie do pojęcia cyberzagrożeń i ich podstawowej klasyfikacji.

10:00 - 11:30 MODUŁ II: Pliki i foldery oraz zarządzanie danymi w duchu GOZ.

1. Struktura drzewa plików - organizacja danych.
2. Tworzenie, kopiowanie, przenoszenie i usuwanie plików.
3. Różnica między usuwaniem a trwałym usuwaniem danych (bezpieczeństwo danych).
4. Praca z pamięcią zewnętrzną - bezpieczne użytkowanie.
5. Zarządzanie cyklem życia danych - ograniczanie e-odpadów i nadmiaru plików.
6. Kompresja danych i archiwizacja jako element redukcji zużycia zasobów.

11:30 - 13:00 MODUŁ III: Przeglądarka i wyszukiwarka - bezpieczne i świadome korzystanie z sieci.

1. Wybór przeglądarki (Edge, Chrome, Brave) pod kątem prywatności, bezpieczeństwa i obciążenia systemu.
2. Świadome korzystanie z wyszukiwarki - ograniczanie zbędnych zapytań i danych.
3. Zakładki, historia i organizacja pracy. Zarządzanie kartami i rozszerzeniami jako element optymalizacji zużycia zasobów.

4. Bezpieczne pobieranie plików. Jak bezpiecznie pobierać PDFy i obrazy z sieci, nie instalując przypadkiem zbędnych programów.
5. Podstawy detekcji zagrożeń w Internecie (fałszywe strony, złośliwe pliki).

13:00 - 13:45 Przerwa.

13:45 - 15:00 MODUŁ IV: Wiarygodność w sieci i HTTPS. Identyfikacja zagrożeń.

1. Anatomia adresu WWW i domeny. Co mówi nam nazwa domeny i dlaczego końcówka (.pl, .com, .gov.pl) ma znaczenie.
2. Symbol kłódki i protokół HTTPS - dlaczego szyfrowanie jest kluczowe przy płatnościach i logowaniu.
3. Metody identyfikacji zagrożeń (fałszywe strony, phishing).
4. Weryfikacja źródeł informacji jako element odpowiedzialnego korzystania z Internetu.
5. Rola bezpieczeństwa danych w ochronie użytkownika i organizacji.

15:00 - 16:30 MODUŁ V: Komunikacja i chmura - bezpieczne zarządzanie danymi.

1. Poczta e-mail - bezpieczne korzystanie i rozpoznawanie zagrożeń.
2. Wprowadzenie do chmury (Google Drive). Dobre praktyki korzystania z chmury: porządkowanie danych, ograniczanie duplikatów.
3. Przechowywanie danych a bezpieczeństwo i energooszczędność.
4. Porównanie: dane lokalne vs chmura.
5. Wprowadzenie do monitorowania danych i ich przepływu.

II DZIEŃ SZKOLENIA [część teoretyczna: 1,5 godziny, część praktyczna: 4,5 godziny, przerwa: 45 min, kwestie organizacyjne: 30 min, walidacja oraz egzamin: 45 min] - 01.07.2026:

08:30 - 08:45 Przywitanie uczestników, krótkie przypomnienie materiału z poprzedniego dnia, sprawdzenie i rozwiązanie ewentualnych trudności na aktualnym etapie szkolenia.

08:45 - 10:00 MODUŁ VI: Cyberzagrożenia i socjotechnika. Komunikacja bezpieczeństwa.

1. Psychologia oszustwa - dlaczego dajemy się nabrać? (presja czasu, strach, obietnica zysku).
2. Phishing, smishing, vishing - rozpoznawanie zagrożeń: podejrzanych maili, SMS-ów i telefonów od „konsultantów bankowych”. Wpływ cyberataków na zużycie zasobów i energii
3. Metody detekcji zagrożeń w praktyce.
4. Jak komunikować zagrożenia innym użytkownikom.
5. Analiza przypadków i wspólne ćwiczenia.

10:00 - 11:30 MODUŁ VII: Twierdza haseł i tożsamość cyfrowa. Zarządzanie bezpieczeństwem.

1. Hasła i frazy hasłowe - dlaczego długość jest ważniejsza niż skomplikowanie?
2. Menedżery haseł - konfiguracja.
3. Uwierzytelnianie wieloskładnikowe (2FA) - dlaczego samo hasło to dziś za mało i jak użyć telefonu jako klucza. Zarządzanie dostępem jako element odpowiedzialnego zarządzania systemami IT.
4. Wycieki danych - analiza i reagowanie (Have I Been Pwned).
5. Zarządzanie bezpieczeństwem użytkownika jako element ograniczania ryzyka incydentów generujących straty zasobów.

11:30 - 13:00 MODUŁ VIII: Era AI - możliwości, zagrożenia i rozwój kompetencji.

1. AI w codziennym życiu - jak AI pomaga w wyszukiwarkach i nawigacji.
2. ChatGPT, Google Gemini i asystenci - wykorzystanie AI do pisania pism, streszczania tekstów czy tłumaczeń. Metody ograniczania nadmiarowych zapytań i generacji.
3. Zagrożenia nowej ery - deepfake (fałszywe wideo/głos) - jak nie dać się oszukać na „klonowanie głosu” bliskiej osoby.
4. Rola ciągłego uczenia się w cyberbezpieczeństwie.
5. Wykorzystanie AI w wykrywaniu zagrożeń i optymalizacji systemów bezpieczeństwa.

13:00 - 13:45 Przerwa.

13:45 - 14:45 MODUŁ IX: Prywatność i bezpieczeństwo sieciowe. Optymalizacja infrastruktury.

1. Bezpieczne Wi-Fi i konfiguracja routera.
2. Zagrożenia publicznych sieci.
3. VPN - działanie i wpływ na bezpieczeństwo. Kiedy warto ukryć swoją aktywność i jak działają blokery reklam (uBlock Origin).
4. Narzędzia ochrony prywatności. VirusTotal - praktyczne narzędzie do sprawdzania podejrzanych plików przed ich otwarciem.
5. Optymalizacja zużycia zasobów w sieci i systemach bezpieczeństwa.

14:45 - 15:30 MODUŁ X: Cyfrowy minimalizm i eko-użytkownik. Zarządzanie sprzętem.

1. Zarządzanie danymi i redukcja śladu cyfrowego.

2. Wpływ przechowywania danych na środowisko.
3. Recykling sprzętu i bezpieczne usuwanie danych. Second life sprzętu - jak przygotować stary komputer do oddania/sprzedaży (trwałe niszczenie danych). GOZ w praktyce IT.
4. Aktualizacje - dlaczego „łatanie" systemu to najważniejszy nawyk bezpiecznego użytkownika
5. Cykl życia sprzętu IT i ograniczanie e-odpadów.
6. Dobre praktyki eko w codziennym korzystaniu z technologii.

15:30 - 15:45 Podsumowanie szkolenia, sesja pytań, przeprowadzenie post-testów.

15:45 - 16:30 Walidacja (analiza dowodów i deklaracji) i egzamin - test teoretyczny online.

***UWAGI DOTYCZĄCE WALIDACJI:**

Walidacja **przeprowadzana jest w formie ZDALNEJ** [forma zdalna dotyczy tylko i wyłącznie instytucji walidującej i certyfikującej - uczestnicy wypełniają test i realizują ćwiczenia, będąc na sali szkoleniowej] - i podzielona jest na 2 etapy:

- walidację **części praktycznej:** uczestnicy podczas szkolenia wykonują ćwiczenia, pod koniec szkolenia zostają one przesłane do weryfikacji przez instytucję zewnętrzną (analiza dowodów i deklaracji).
- walidację **części teoretycznej:** uczestnicy pod koniec szkolenia wypełniają elektroniczny test teoretyczny, który zostaje przygotowany i przesłany przez instytucję zewnętrzną, na podstawie efektów uczenia się określonych w zakresie kwalifikacji).

Harmonogram

Liczba przedmiotów/zajęć: 16

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 16 Przywitanie uczestników, omówienie szkolenia, przeprowadzenie pre-testów w celu oceny początkowego poziomu wiedzy uczestników.	Kamil Urbacz	30-06-2026	08:30	08:45	00:15
2 z 16 MODUŁ I: Anatomia komputera. Wprowadzenie do cyberbezpieczeństwa i eko-IT.	Kamil Urbacz	30-06-2026	08:45	10:00	01:15
3 z 16 MODUŁ II: Pliki i foldery oraz zarządzanie danymi w duchu GOZ.	Kamil Urbacz	30-06-2026	10:00	11:30	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
4 z 16 MODUŁ III: Przeglądarka i wyszukiwarka - bezpieczne i świadome korzystanie z sieci.	Kamil Urbacz	30-06-2026	11:30	13:00	01:30
5 z 16 Przerwa.	Kamil Urbacz	30-06-2026	13:00	13:45	00:45
6 z 16 MODUŁ IV: Wiarygodność w sieci i HTTPS. Identyfikacja zagrożeń.	Kamil Urbacz	30-06-2026	13:45	15:00	01:15
7 z 16 MODUŁ V: Komunikacja i chmura - bezpieczne zarządzanie danymi.	Kamil Urbacz	30-06-2026	15:00	16:30	01:30
8 z 16 Przywitanie uczestników, krótkie przypomnienie materiału z poprzedniego dnia, sprawdzenie i rozwiązanie ewentualnych trudności na aktualnym etapie szkolenia.	Kamil Urbacz	01-07-2026	08:30	08:45	00:15
9 z 16 MODUŁ VI: Cyberzagrożenia i socjotechnika. Komunikacja bezpieczeństwa.	Kamil Urbacz	01-07-2026	08:45	10:00	01:15
10 z 16 MODUŁ VII: Twierdza haseł i tożsamość cyfrowa. Zarządzanie bezpieczeństwem.	Kamil Urbacz	01-07-2026	10:00	11:30	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
11 z 16 MODUŁ VIII: Era AI - możliwości, zagrożenia i rozwój kompetencji.	Kamil Urbacz	01-07-2026	11:30	13:00	01:30
12 z 16 Przerwa.	Kamil Urbacz	01-07-2026	13:00	13:45	00:45
13 z 16 MODUŁ IX: Prywatność i bezpieczeństwo sieciowe. Optymalizacja infrastruktury.	Kamil Urbacz	01-07-2026	13:45	14:45	01:00
14 z 16 MODUŁ X: Cyfrowy minimalizm i eko-użytkownik. Zarządzanie sprzętem.	Kamil Urbacz	01-07-2026	14:45	15:30	00:45
15 z 16 Podsumowanie szkolenia, sesja pytań, przeprowadzenie post-testów.	Kamil Urbacz	01-07-2026	15:30	15:45	00:15
16 z 16 Walidacja (analiza dowodów i deklaracji) i egzamin - test teoretyczny online.	-	01-07-2026	15:45	16:30	00:45

Cennik

Jeżeli korzystasz z dofinansowania w wysokości co najmniej 70% przysługuje Tobie zwolnienie z podatku VAT

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	6 081,12 PLN

Koszt przypadający na 1 uczestnika netto	4 944,00 PLN
Koszt osobogodziny brutto	380,07 PLN
Koszt osobogodziny netto	309,00 PLN
W tym koszt walidacji brutto	150,00 PLN
W tym koszt walidacji netto	121,95 PLN
W tym koszt certyfikowania brutto	200,00 PLN
W tym koszt certyfikowania netto	162,60 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Kamil Urbacz

Informatyk, projektant energooszczędnych stron internetowych, ekspert w dziedzinie green marketingu oraz doświadczony trener z wieloletnią praktyką w dziedzinie technologii cyfrowych. Od 2017 roku nieustannie zdobywa doświadczenie w programowaniu i projektowaniu stron i aplikacji webowych (m.in. HTML, Python, WordPress, CSS, Java).

Jako ekspert specjalizuje się w obszarach: generatywnej sztucznej inteligencji i projektowaniu stron internetowych zgodnych z zasadami no-code. Kładzie nacisk na przekazywanie praktycznych umiejętności, dzięki czemu uczestnicy zdobywają wiedzę gotową do natychmiastowego wdrożenia, co stanowi realne wsparcie w ich rozwoju zawodowym.

Doświadczenie zawodowe lub kwalifikacje zdobyte nie wcześniej niż 5 lat przed datą wprowadzenia usługi: m.in.: PARP - Komunikacja marketingowa (2021), PARP - Cyberbezpieczeństwo w MŚP (2021), Google - Podstawy marketingu internetowego (2021), IT & Desktop Computer Support (2021), Google - Foundations of User Experience (UX) Design (2021), Google - Crash Course of Python (2022), Google - Technical Support Fundamentals (2022), Poznaj AI - Praktyka, narzędzia, ciekawostki (2025), Oracle Certified Associate Java Programmer (2025), Climate Change: From Learning to Action (UN-CC Learn, 2025), How to prevent e-waste? (UN-CC Learn, 2025), Gemini Certified Educator (2025), Google & SGH: Wykorzystanie AI w rozwoju firmy (2025).

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy Uczestnik otrzyma **konspekt z materiałami w wersji drukowanej**, który zdecydowanie ułatwia pracę podczas szkolenia, a także posłuży utrwaleniu wiadomości po odbytym szkoleniu. Zapewniamy także notesy i długopisy. Dla chętnych udostępniamy również konspekt w wersji cyfrowej.

Informacje dodatkowe

Kontakt do osoby prowadzącej usługę: kamil.urbacz@simply.edu.pl

Uprzejmie prosimy uczestników **o zabranie ze sobą laptopa**. W przypadku braku dostępu do wymienionego sprzętu lub niemożności jego zabrania na szkolenie, **prosimy o wcześniejsze poinformowanie Dostawcy Usługi.** Dostawca ma możliwość zapewnienia sprzętu **dla każdego Uczestnika**.

Możliwość zwolnienia z VAT na podstawie: Dz.U. 2013 poz. 1722 (Rozporządzenie Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień) §3, ust. 1, pkt 14.

Adres

ul. Żorska 14

44-200 Rybnik

woj. śląskie

Centrum biznesowe "Żorska14". Ogólnodostępny parking przy budynku.

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi

Kontakt

Maria Szymak

E-mail maria.szymak@simply.edu.pl

Telefon (+48) 721 324 130