Możliwość dofinansowania

Digital Marketing
Krzysztof Szymak

★★★★★ 4,9 / 5

535 ocen

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

Numer usługi 2026/04/28/163842/3518468

Skrbeńsko
Usługa szkoleniowa
stacjonarna
Zajęcia grupowe
16:00 h
08.07.2026 do 15.07.2026

6 081,12 PLN brutto
4 944,00 PLN netto
380,07 PLN brutto/h
309,00 PLN netto/h
233,33 PLN cena rynkowa

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/ICVC Specjalista ds. cyberbezpieczeństwa (ICVC/CBB 207771.19).** 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	07-07-2026
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 przygotowuje uczestnika do samodzielnego, bezpiecznego i odpowiedzialnego korzystania z technologii ICT w pracy z komputerem, Internetem, pocztą, chmurą i narzędziami AI, a także organizacji danych, rozpoznawania cyberzagrożeń, ochrony prywatności i tożsamości cyfrowej oraz stosowania zasad eko-IT, GOZ i cyfrowego minimalizmu ograniczających ślad środowiskowy.

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
Charakteryzuje podstawy działania komputera oraz technologii ICT.	Wyjaśnia rolę podstawowych elementów komputera, takich jak procesor, pamięć RAM, dysk i system operacyjny.	Test teoretyczny
	Rozróżnia sprzęt, oprogramowanie, system operacyjny, przeglądarkę internetową i usługi chmurowe.	Test teoretyczny
	Wskazuje wpływ pracy urządzeń cyfrowych, serwerów i przechowywania danych na zużycie energii oraz emisję CO_2.	Test teoretyczny
Wyjaśnia zasady organizacji danych zgodnie z zasadami bezpieczeństwa i eko-IT.	Opisuje zasady tworzenia logicznej struktury plików i folderów.	Test teoretyczny
	Rozróżnia usuwanie danych, trwałe usuwanie danych, archiwizację i kompresję plików.	Test teoretyczny
	Wskazuje znaczenie ograniczania nadmiaru danych, duplikatów i zbędnych plików dla redukcji śladu cyfrowego.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozpoznaje zagrożenia związane z korzystaniem z Internetu, poczty elektronicznej i usług cyfrowych.	Rozróżnia phishing, smishing, vishing, fałszywe strony internetowe, złośliwe pliki i próby wyłudzenia danych.	Test teoretyczny
	Wskazuje elementy świadczące o wiarygodności strony internetowej, w tym domenę, protokół HTTPS i symbol kłódki.	Test teoretyczny
	Opisuje zasady bezpiecznego pobierania plików, korzystania z poczty elektronicznej i weryfikowania źródeł informacji.	Test teoretyczny
Omawia zasady ochrony tożsamości cyfrowej, prywatności i dostępu do kont.	Wyjaśnia znaczenie silnych haseł, fraz hasłowych, menedżerów haseł i uwierzytelniania wieloskładnikowego.	Test teoretyczny
	Wskazuje ryzyka związane z wyciekiem danych, korzystaniem z publicznych sieci Wi-Fi i nadmiernym udostępnianiem informacji.	Test teoretyczny
	Opisuje zastosowanie narzędzi wspierających bezpieczeństwo i prywatność, takich jak VPN, blokery reklam, Have I Been Pwned i VirusTotal.	Test teoretyczny
Charakteryzuje możliwości i zagrożenia związane z wykorzystaniem AI w środowisku cyfrowym z uwzględnieniem zasad zrównoważonego rozwoju.	Wskazuje przykłady zastosowania AI w codziennym korzystaniu z technologii, w tym do pisania, streszczania, tłumaczenia i wyszukiwania informacji.	Test teoretyczny
	Rozpoznaje zagrożenia związane z AI, w tym deepfake, klonowanie głosu, dezinformację i nieuprawnione przetwarzanie danych.	Test teoretyczny z wynikiem generowanym automatycznie
	Wyjaśnia znaczenie precyzyjnego formułowania zapytań do AI jako sposobu ograniczania zbędnych generacji i nadmiernego zużycia zasobów cyfrowych.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Organizuje dane cyfrowe zgodnie z zasadami bezpieczeństwa, porządku i eko-IT.	Tworzy strukturę folderów odpowiadającą wskazanemu celowi pracy.	Analiza dowodów i deklaracji
	Porządkuje pliki poprzez zapisanie, przeniesienie, usunięcie lub skompresowanie wskazanych danych.	Analiza dowodów i deklaracji
	Ogranicza nadmiar danych poprzez usunięcie duplikatów lub zbędnych plików roboczych.	Analiza dowodów i deklaracji
Korzysta z Internetu i poczty elektronicznej w sposób bezpieczny i świadomy.	Weryfikuje wiarygodność strony internetowej na podstawie adresu, domeny i protokołu HTTPS.	Analiza dowodów i deklaracji
	Sprawdza podejrzany plik, link lub adres e-mail za pomocą narzędzia wspierającego bezpieczeństwo cyfrowe.	Analiza dowodów i deklaracji
Stosuje podstawowe zabezpieczenia kont, urządzeń i danych.	Konfiguruje silne hasła lub frazy hasłowe.	Analiza dowodów i deklaracji
	Uruchamia uwierzytelnienie wieloskładnikowe dla wybranej usługi.	Analiza dowodów i deklaracji
Wykorzystuje narzędzia cyfrowe i AI w sposób odpowiedzialny środowiskowo.	Przygotowuje precyzyjne zapytanie do narzędzia AI w celu wykonania określonego zadania tekstowego.	Analiza dowodów i deklaracji
	Ogranicza liczbę nadmiarowych zapytań do AI poprzez doprecyzowanie celu, kontekstu i oczekiwanego formatu odpowiedzi.	Analiza dowodów i deklaracji
	Wskazuje działanie zmniejszające ślad cyfrowy podczas pracy z chmurą, przeglądarką, plikami lub narzędziami AI.	Analiza dowodów i deklaracji
Uzasadnia znaczenie odpowiedzialnego i bezpiecznego zachowania w środowisku cyfrowym.	Wskazuje konsekwencje nieostrożnego otwierania linków, załączników lub udostępniania danych w sieci.	Test teoretyczny
	Wyjaśnia znaczenie informowania innych użytkowników o podejrzanych wiadomościach, fałszywych stronach lub próbach wyłudzenia danych.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uzasadnia znaczenie zrównoważonego korzystania z technologii ICT.	Wskazuje wpływ nadmiarowego przechowywania danych, zbędnych zapytań i e-odpadów na środowisko.	Test teoretyczny
	Wyjaśnia znaczenie cyfrowego minimalizmu, eko-IT i GOZ w codziennym korzystaniu z komputera, Internetu, chmury i narzędzi AI.	Test teoretyczny
Identyfikuje zasady współpracy z innymi użytkownikami w środowisku cyfrowym w sposób odpowiedzialny i efektywny.	Wskazuje zasady współdzielenia plików i pracy zespołowej w chmurze.	Test teoretyczny
	Wyjaśnia znaczenie jasnego podziału zadań i odpowiedzialności w pracy zespołowej online.	Test teoretyczny
Charakteryzuje sposoby jasnej, uprzejmej i adekwatnej do sytuacji komunikacji w środowisku cyfrowym.	Wskazuje zasady poprawnej komunikacji w e-mailach, komunikatorach i podczas spotkań online.	Test teoretyczny
	Wyjaśnia znaczenie dostosowania formy komunikatu do odbiorcy i kontekstu sytuacyjnego.	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

Strona internetowa Instytucji Walidującej: https://icvc.eu

Informacje

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

Program

Usługa prowadzi do nabycia kwalifikacji międzynarodowej: **GCCS/ICVC Specjalista ds. cyberbezpieczeństwa (ICVC/CBB 207771.19).**

W ramach szkolenia realizujemy rozszerzoną wersję kwalifikacji GCCS/ICVC - uwzględniającą umiejętności warsztatowe z bezpiecznego i odpowiedzialnego korzystania z komputera oraz Internetu, a także obejmującą zasady zrównoważonego rozwoju, odpowiedzialności za środowisko i zielonej gospodarki, zgodne z ramami Europejskiego Zielonego Ładu i ESG.

Szkolenie stanowi odpowiedź na cele i kierunki rozwoju wskazane w **Regionalnej Strategii Innowacji Województwa Śląskiego 2030 (RIS WSL 2030)**, w szczególności w obszarach inteligentnych specjalizacji:

- OBSZAR TECHNOLOGICZNY - TECHNOLOGIE INFORMACYJNE I TELEKOMUNIKACYJNE: **4.2. Technologie informacyjne**

Zakres szkolenia wpisuje się w Priorytetowe Technologie Rozwojowe (**PRT**) wskazane w **Regionalnej Strategii Innowacji Województwa Śląskiego 2030** oraz **Programie Rozwoju Technologii Województwa Śląskiego 2019-2030**, w szczególności w obszary:

1. Technologie informacyjno-komunikacyjne (ICT),
2. Technologie cyfrowe wspierające transformację przedsiębiorstw,
3. Technologie związane ze zrównoważonym rozwojem i zieloną transformacją,
4. Technologie multimedialne i kreatywne,
5. Sztuczna inteligencja i analiza danych.

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.

!!! WAŻNE: Szkolenie realizowane jest w terminie 08-09.07.2026 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 08-15.07.2026, ponieważ obejmuje:**

- **okres prowadzenia szkolenia (8-9 lipca)**
- **oraz okres oczekiwania na wynik walidacji (do 15 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] - 08.07.2026:

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] - 09.07.2026:

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 oraz test teoretyczny online (egzamin).

***UWAGI DOTYCZĄCE WALIDACJI:**

Walidacja (test teoretyczny online oraz analiza dowodów i deklaracji) określona jest w harmonogramie w ostatniej pozycji "Walidacja" w postaci jednego punktora i trwa łącznie 45 minut. 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, gromadząc tym samym dowody pracy własnej i nabycia efektów uczenia się prowadzących do zdobycia umiejętności, 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 karcie usługi (test teoretyczny online).

Warunki organizacyjne dla przeprowadzenia usługi: szkolenie będzie realizowane w formie warsztatowej, z wykorzystaniem **indywidualnych stanowisk komputerowych**. Każdy uczestnik będzie pracował **samodzielnie** przy komputerze, wykonując ćwiczenia z zakresu prompt engineeringu, generatywnej AI, analizy danych, tworzenia treści, grafik, audio/wideo oraz automatyzacji wybranych procesów marketingowych.

Każdy uczestnik wykonuje ćwiczenia praktyczne **indywidualnie**, przy bieżącym wsparciu trenera. Sala szkoleniowa będzie wyposażona w dostęp do Internetu/Wi-Fi oraz zasilania umożliwiającego pracę na komputerach przez cały czas trwania zajęć.

Harmonogram

Liczba pozycji harmonogramu: 16

Przedmiot / temat	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	08-07-2026	08:30	08:45	00:15

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
2 z 16 MODUŁ I: Anatomia komputera. Wprowadzenie do cyberbezpieczeństwa i eko-IT.	Kamil Urbacz	08-07-2026	08:45	10:00	01:15
3 z 16 MODUŁ II: Pliki i foldery oraz zarządzanie danymi w duchu GOZ.	Kamil Urbacz	08-07-2026	10:00	11:30	01:30
4 z 16 MODUŁ III: Przeglądarka i wyszukiwarka - bezpieczne i świadome korzystanie z sieci.	Kamil Urbacz	08-07-2026	11:30	13:00	01:30
5 z 16 Przerwa.	Kamil Urbacz	08-07-2026	13:00	13:45	00:45
6 z 16 MODUŁ IV: Wiarygodność w sieci i HTTPS. Identyfikacja zagrożeń.	Kamil Urbacz	08-07-2026	13:45	15:00	01:15
7 z 16 MODUŁ V: Komunikacja i chmura - bezpieczne zarządzanie danymi.	Kamil Urbacz	08-07-2026	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	09-07-2026	08:30	08:45	00:15

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
9 z 16 MODUŁ VI: Cyberzagrożenia i socjotechnika. Komunikacja bezpieczeństwa.	Kamil Urbacz	09-07-2026	08:45	10:00	01:15
10 z 16 MODUŁ VII: Twierdza haseł i tożsamość cyfrowa. Zarządzanie bezpieczeństwem.	Kamil Urbacz	09-07-2026	10:00	11:30	01:30
11 z 16 MODUŁ VIII: Era AI - możliwości, zagrożenia i rozwój kompetencji.	Kamil Urbacz	09-07-2026	11:30	13:00	01:30
12 z 16 Przerwa.	Kamil Urbacz	09-07-2026	13:00	13:45	00:45
13 z 16 MODUŁ IX: Prywatność i bezpieczeństwo sieciowe. Optymalizacja infrastruktury.	Kamil Urbacz	09-07-2026	13:45	14:45	01:00
14 z 16 MODUŁ X: Cyfrowy minimalizm i eko-użytkownik. Zarządzanie sprzętem.	Kamil Urbacz	09-07-2026	14:45	15:30	00:45
15 z 16 Podsumowanie szkolenia, sesja pytań, przeprowadzenie post-testów.	Kamil Urbacz	09-07-2026	15:30	15:45	00:15
16 z 16 Walidacja (analiza dowodów i deklaracji) i egzamin - test teoretyczny online.	-	09-07-2026	15:45	16:30	00:45

Cennik

Jeżeli korzystasz z dofinansowania i usługa stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego wraz z usługą lub dostawą towarów ściśle związaną z usługami kształcenia zawodowego lub przekwalifikowania zawodowego to możesz mieć możliwość skorzystania za zwolnienia z podatku VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2024 r. o podatku od towarów i usług, jeśli usługa w całości jest finansowana ze środków publicznych lub § 3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień w przypadku, gdy usługa jest finansowana w co najmniej 70% ze środków publicznych.

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	100,00 PLN
W tym koszt walidacji netto	81,30 PLN
W tym koszt certyfikowania brutto	150,00 PLN
W tym koszt certyfikowania netto	121,95 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. Zielona 25
44-341 Skrbeńsko
woj. śląskie

Ośrodek Kultury Skrbeńsko. 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