Możliwość dofinansowania

Specjalista ds. cyberbezpieczeństwa w zielonej transformacji cyfrowej - szkolenie kończące się egzaminem i uzyskaniem kwalifikacji.

Numer usługi 2026/07/26/51191/3710216

5 739,18 PLN brutto
4 666,00 PLN netto
358,70 PLN brutto/h
291,63 PLN netto/h
261,33 PLN cena rynkowa

NEXTDAY spółka z ograniczoną odpowiedzialnością

4,8 / 5

3 226 ocen

Wisła
Usługa szkoleniowa
stacjonarna
Zajęcia grupowe
16:00 h
10.10.2026 do 21.10.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Usługa skierowana jest do dorosłych uczestników, w szczególności: • osoby chcące zdobyć kompetencje w zakresie cyberbezpieczeństwa i ochrony danych • osoby odpowiedzialne za bezpieczeństwo informacji w firmach i instytucjach • osoby zainteresowane zieloną transformacją cyfrową i energooszczędnymi technologiami IT • osoby planujące rozwój zawodowy w branży cyberbezpieczeństwa • osoby chcące zdobyć kwalifikacje z zakresu cyberbezpieczeństwa i zrównoważonych technologii IT • wszystkich osób zainteresowanych nabyciem umiejętności w zakresie cyberbezpieczeństwa i ochrony danych. Do udziału w szkoleniu nie jest wymagane wykształcenie kierunkowe ani doświadczenie zawodowe w obszarze cyberbezpieczeństwa. Uczestnik powinien posiadać podstawowe kompetencje cyfrowe oraz podstawową znajomość funkcjonowania środowiska IT, obejmującą obsługę systemu operacyjnego, plików, aplikacji internetowych i podstawowych pojęć z zakresu bezpieczeństwa informacji.
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	09-10-2026
Forma prowadzenia usługi	stacjonarna

Cel

Cel edukacyjny

Usługa przygotowuje uczestników do nabycia zielonych kompetencji w obszarze cyberbezpieczeństwa i bezpieczeństwa informacji, w tym ograniczanie zużycia energii, nadmiernego wykorzystania zasobów cyfrowych i ilości e-odpadów. Uczestnik nabywa umiejętności identyfikowania zagrożeń, monitorowania infrastruktury IT, analizy logów oraz zarządzania cyklem życia oprogramowania i infrastruktury z uwzględnieniem efektywności zasobowej. Usługa kończy się nabyciem kwalifikacji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozróżnia rodzaje zagrożeń cyberbezpieczeństwa, dobiera metody ich identyfikacji oraz ocenia ich wpływ na bezpieczeństwo i efektywne wykorzystanie zasobów infrastruktury IT	Wymienia co najmniej 5 rodzajów zagrożeń cyberbezpieczeństwa i wskazuje ich możliwy wpływ na ciągłość działania oraz wykorzystanie zasobów IT.	Test teoretyczny
	Opisuje metody detekcji zagrożeń z wykorzystaniem narzędzi monitorowania infrastruktury sieciowej i analizy logów.	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, standardy i zasady ochrony danych oraz bezpieczeństwa informacji z uwzględnieniem odpowiedzialnego i zasobooszczędnego przetwarzania danych	Wymienia obowiązujące regulacje prawne w zakresie ochrony danych osobowych.	Test teoretyczny
	Opisuje standardy i środki ochrony informacji oraz wskazuje zasady ograniczania nadmiarowego przechowywania i przetwarzania danych.	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

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Konfiguruje podstawowe funkcje systemu monitorowania ruchu sieciowego z uwzględnieniem zasad efektywności energetycznej.	Przygotowuje rozwiązanie monitorowania ruchu sieciowego minimalizujące zużycie energii	Obserwacja w warunkach symulowanych
	Dokumentuje proces konfiguracji systemu z analizą redukcji obciążenia infrastruktury	Obserwacja w warunkach symulowanych
Opracowuje zasady bezpiecznego i zasobooszczędnego postępowania z danymi oraz komunikowania ich pracownikom.	Przygotowuje zestaw zasad dotyczących bezpiecznego postępowania z danymi i reagowania na cyberzagrożenia	Obserwacja w warunkach symulowanych
	Uwzględnia w przygotowanych zasadach ograniczenie zbędnego przetwarzania danych, dokumentacji papierowej i wykorzystania zasobów cyfrowych.	Obserwacja w warunkach symulowanych
Analizuje sposób przechowywania logów bezpieczeństwa i opracowuje proces archiwizacji z wykorzystaniem kompresji.	Analizuje istniejący sposób przechowywania logów i identyfikuje możliwości optymalizacji.	Obserwacja w warunkach symulowanych
	Opracowuje procedurę archiwizacji danych zgodną z wymogami prawnymi i zasadami efektywnego wykorzystania zasobów.	Obserwacja w warunkach symulowanych
Planuje działania dotyczące cyklu życia oprogramowania z uwzględnieniem open-source i długoterminowego wsparcia.	Planuje strategię aktualizacji oprogramowania ograniczającą niepotrzebną wymianę sprzętu.	Obserwacja w warunkach symulowanych
	Dokumentuje ocenę oprogramowania open-source w kontekście bezpieczeństwa i ekologii.	Obserwacja w warunkach symulowanych
Promuje zasady etyki zawodowej i odpowiedzialności zasobowej w komunikacji z zespołem IT	Demonstruje świadome podejście do zasobów poprzez wspieranie inicjatyw zielonego cyberbezpieczeństwa	Obserwacja w warunkach symulowanych
	Komunikuje znaczenie zrównoważonego rozwoju w kontekście działań bezpieczeństwa informacji	Obserwacja w warunkach symulowanych
Współpracuje interdyscyplinarnie z działami IT, kadrami i kadrą zarządzającą w celu realizacji celów ekologicznych	Koordynuje projekty bezpieczeństwa z uwzględnieniem wymogów zrównoważonego rozwoju	Obserwacja w warunkach symulowanych
	Konsultuje decyzje techniczne z pracownikami różnych departamentów w sprawie zasobów	Obserwacja w warunkach symulowanych

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Ocenia skuteczność działań bezpieczeństwa pod względem zarówno ochrony, jak i efektywności	Analizuje metryki bezpieczeństwa i wskaźniki zużycia energii w procesach ochrony danych	Obserwacja w warunkach symulowanych
	Rekomenduje działania usprawniające opierające się na zbalansowaniu bezpieczeństwa i ekologii	Obserwacja w warunkach symulowanych
Doskonali umiejętności rozwiązywania konfliktów między wymogami bezpieczeństwa a zielonymi celami	Opracowuje strategie negocjacji w przypadku sprzeczności między ochroną danych a efektywnością	Obserwacja w warunkach symulowanych
	Znajduje kompromisowe rozwiązania łączące wysokie standardy bezpieczeństwa z praktykami ekologicznymi	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://standardgccs.com/qualifications/

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

Informacje

Nazwa Podmiotu prowadzącego walidację	ICVC CERTYFIKACJA SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ
Nazwa Podmiotu certyfikującego	Talent Odyssey Ltd (Global Competence Certification Standard)

Program

Kwalifikacje:

Usługa prowadzi do uzyskania kwalifikacji SPECJALISTA DS. CYBERBEZPIECZEŃSTWA nadawanej przez międzynarodowy podmiot certyfikujący.

Sposób walidacji i egzamin

Walidacja obejmuje test teoretyczny oraz obserwację w warunkach symulowanych.

Test teoretyczny służy weryfikacji efektów uczenia się z zakresu wiedzy. Warunkiem zaliczenia tej części jest uzyskanie minimum 70% poprawnych odpowiedzi.

W ramach obserwacji w warunkach symulowanych uczestnik realizuje zadanie według jednolitego scenariusza przygotowanego przez podmiot walidujący. Walidator obserwuje wykonanie poszczególnych czynności, w tym konfigurację monitoringu ruchu sieciowego, analizę i archiwizację logów, opracowanie zasad bezpiecznego i zasobooszczędnego postępowania z danymi, planowanie aktualizacji i wykorzystania oprogramowania open-source, ocenę rozwiązań pod kątem bezpieczeństwa i ekologii, analizę wskaźników bezpieczeństwa i zużycia energii, współpracę, koordynowanie działań i konsultowanie decyzji z przedstawicielami różnych działów oraz wypracowanie kompromisu pomiędzy wymaganiami bezpieczeństwa a celami środowiskowymi. Każda czynność oceniana jest odrębnie zgodnie z kryteriami wskazanymi w karcie usługi.

Każdy uczestnik zapisuje wyniki zadania w indywidualnym arkuszu. Walidator obserwuje przebieg realizacji oraz ocenia rezultat każdego uczestnika na podstawie jednolitego arkusza obserwacji i wcześniej określonych kryteriów. Równoległa realizacja zadania, wykorzystanie przygotowanego środowiska symulowanego, gotowych zestawów danych oraz jednolitego arkusza oceny umożliwiają przeprowadzenie rzetelnej walidacji w czasie 1 godziny i 45 minut.

Warunkiem pozytywnego wyniku części praktycznej jest uzyskanie min. 70% wszystkich kryteriów, przy czym obowiązkowe jest spełnienie wszystkich kryteriów odnoszących się do zielonych kompetencji. Po spełnieniu warunków otrzymuje certyfikat potwierdzający uzyskanie kwalifikacji.

Czas oczekiwania na wynik walidacji oraz na dokument wystawiany przez uprawniony podmiot certyfikujący wynosi do 8 dni roboczych od dnia egzaminu.

Realizacja szkolenia: 10-11.10. 2026 r.

Oczekiwanie na wynik walidacji oraz dokumentu - do 21.10.2026 r.

Powiązanie z RSI 2030

Usługa wpisuje się w Regionalną Strategię Innowacji Województwa Śląskiego 2030 „Inteligentne Śląskie” w obszarze inteligentnej specjalizacji, „Technologie informacyjne i komunikacyjne” oraz „Zielona gospodarka”, poprzez rozwój kompetencji związanych z cyberbezpieczeństwem, ochroną danych, transformacją cyfrową oraz wdrażaniem energooszczędnych i zrównoważonych rozwiązań IT wspierających odpowiedzialną transformację przedsiębiorstw.

Powiązanie z PRT WSL 2019–2030

Usługa realizuje podobszar **4.2 Technologie informacyjne** poprzez rozwój umiejętności związanych z monitorowaniem infrastruktury IT, analizą ruchu sieciowego i logów, optymalizacją wykorzystania zasobów cyfrowych, archiwizacją danych oraz zarządzaniem cyklem życia oprogramowania i infrastruktury.

Usługa realizuje podobszar **4.6 Bezpieczeństwo informacji** poprzez rozwój umiejętności identyfikacji i detekcji zagrożeń, ochrony danych, analizy logów bezpieczeństwa, stosowania zasad i standardów bezpieczeństwa informacji oraz organizacji procesów ochrony danych i infrastruktury.

Powiązanie z ww. podobszarami znajduje odzwierciedlenie również w efektach uczenia się dotyczących identyfikacji zagrożeń, monitorowania infrastruktury, analizy i archiwizacji logów, ochrony informacji oraz optymalizacji wykorzystania zasobów IT.

Warunki organizacyjne:

- usługa realizowana jest w formie warsztatowej z zajęciami praktycznymi, umożliwiających zdobycie umiejętności z zakresu cyberbezpieczeństwa, ochrony danych oraz monitorowania infrastruktury IT,
- szkolenie prowadzone jest w małych grupach, zapewniających indywidualne wsparcie trenera,
- każdy uczestnik ma zapewniony dostęp do stanowiska komputerowego lub możliwość pracy na własnym sprzęcie,
- podczas zajęć wykorzystywane są narzędzia do monitorowania sieci, analizy logów bezpieczeństwa, platformy e-learningowe oraz materiały szkoleniowe w formie cyfrowej,
- zajęcia realizowane są z wykorzystaniem aktywnych metod dydaktycznych, takich jak ćwiczenia praktyczne, analiza przypadków, symulacje incydentów bezpieczeństwa, praca indywidualna i zespołowa,
- warunki organizacyjne wspierają rozwój kompetencji zielonych poprzez promowanie energooszczędnych rozwiązań IT, ograniczania e-odpadów, efektywnego wykorzystania zasobów cyfrowych oraz zasad zrównoważonego rozwoju,

Ćwiczenia praktyczne realizowane są w przygotowanym środowisku symulowanym, z wykorzystaniem gotowych zestawów logów, danych i scenariuszy incydentów. Uczestnicy nie budują infrastruktury ani systemów bezpieczeństwa od podstaw, lecz wykonują określone zadania analityczne i konfiguracyjne według instrukcji oraz scenariusza przygotowanego przez trenera.

Ćwiczenia, analizy przypadków i scenariusze wykorzystywane podczas szkolenia odnoszą się do realiów przedsiębiorstw produkcyjnych, energetycznych, transportowych, komunalnych oraz podmiotów świadczących usługi cyfrowe. Uwzględniają w szczególności ochronę ciągłości działania, bezpieczeństwo infrastruktury i danych, ograniczanie zużycia energii przez systemy IT, racjonalne przechowywanie danych oraz

wydłużanie cyklu życia sprzętu i oprogramowania.

Usługa realizowana jest w godzinach zegarowych.

Przerwy oraz walidacja efektów uczenia się wliczone są w czas trwania usługi.

ZIELONE KOMPETENCJE

Nadrzędnym celem usługi jest rozwój i nabycie zielonych kompetencji oraz przygotowanie uczestników do uzyskania kwalifikacji związanej z wdrażaniem zasad zrównoważonego rozwoju w obszarze cyberbezpieczeństwa i technologii informacyjnych.

PROGRAM USŁUGI

DZIEŃ I – 9:00–17:00

4,5 h teoria / 2,5 h praktyka / 1 h przerwa

09:00–10:30 – Zielone cyberbezpieczeństwo i rodzaje zagrożeń cyfrowych

Forma: teoria

PRT: 4.2 Technologie informacyjne, 4.6 Bezpieczeństwo informacji

- rodzaje zagrożeń: phishing, malware, ransomware, ataki socjotechniczne,
- identyfikacja i detekcja zagrożeń w systemach IT,
- wpływ incydentów na ciągłość działania, obciążenie infrastruktury i zużycie zasobów,
- monitoring i analiza logów jako narzędzia ograniczania nieefektywnej pracy systemów,
- bezpieczeństwo danych i użytkowników.

10:30–12:00 – Regulacje prawne, bezpieczeństwo informacji i odpowiedzialność cyfrowa

Forma: teoria

PRT: 4.6 Bezpieczeństwo informacji

- RODO i ochrona danych osobowych,
- normy i standardy bezpieczeństwa informacji,
- organizacyjne i technologiczne środki ochrony danych,
- zasobooszczędne przetwarzanie i przechowywanie informacji,
- ograniczanie nadmiarowego gromadzenia danych i dokumentacji papierowej.

12:00–13:00 – Monitorowanie infrastruktury IT, analiza logów i optymalizacja zasobów cyfrowych

Forma: praktyka

PRT: 4.2 Technologie informacyjne, 4.6 Bezpieczeństwo informacji

- analiza ruchu sieciowego i logów bezpieczeństwa,
- identyfikacja nieprawidłowości i zagrożeń,
- monitoring obciążenia infrastruktury IT,
- analiza wpływu obciążenia systemów na zużycie energii,
- optymalizacja wykorzystania zasobów cyfrowych.

13:00–14:00 – Przerwa

14:00–15:30 – Energooszczędna infrastruktura IT i zrównoważone technologie cyfrowe

Forma: teoria

PRT: 4.2 Technologie informacyjne

- wpływ infrastruktury IT na zużycie energii i emisję CO_2,
- energooszczędne rozwiązania w systemach IT i bezpieczeństwie,
- ograniczanie e-odpadów i wydłużanie cyklu życia sprzętu,
- znaczenie długoterminowego wsparcia i rozwiązań open-source,
- ograniczanie śladu cyfrowego organizacji.

15:30–17:00 – Warsztaty praktyczne z zakresu zielonego cyberbezpieczeństwa

Forma: praktyka

PRT: 4.2 Technologie informacyjne, 4.6 Bezpieczeństwo informacji

- konfiguracja narzędzi monitorowania infrastruktury,
- analiza logów i identyfikacja zagrożeń,
- ocena obciążenia systemów i wykorzystania zasobów,
- dobór rozwiązań ograniczających zużycie energii,
- rekomendacje łączące bezpieczeństwo i efektywność zasobową.

DZIEŃ II – 8:00–16:00

2 h 30 min teoria / 2 h 45 min praktyka / 1 h przerwa / 1 h 45 min walidacja

08:00–09:30 – Zarządzanie cyklem życia oprogramowania i ograniczanie e-odpadów

Forma: teoria

PRT: 4.2 Technologie informacyjne

- cykl życia oprogramowania i infrastruktury IT,
- aktualizacje i długoterminowe wsparcie systemów,
- ograniczanie przedwczesnej wymiany sprzętu,
- wykorzystanie open-source w zrównoważonym IT,
- planowanie rozwiązań wydłużających cykl życia infrastruktury.

09:30–10:30 – Ekologiczna archiwizacja danych i optymalizacja zasobów cyfrowych

Forma: teoria

PRT: 4.2 Technologie informacyjne, 4.6 Bezpieczeństwo informacji

- przechowywanie, kompresja i retencja logów,
- ograniczanie nadmiarowego gromadzenia i duplikowania danych,
- efektywne wykorzystanie przestrzeni dyskowej,
- bezpieczna archiwizacja danych,
- ograniczanie śladu cyfrowego poprzez racjonalne zarządzanie danymi.

10:30–12:30 – Warsztaty praktyczne – organizacja procesów zielonego cyberbezpieczeństwa

Forma: praktyka

PRT: 4.2 Technologie informacyjne, 4.6 Bezpieczeństwo informacji

- przygotowanie procedur bezpieczeństwa informacji,
- analiza i optymalizacja sposobu przechowywania danych i logów,
- planowanie działań ograniczających zużycie energii i zasobów IT,
- rozwiązania wspierające dłuższe wykorzystanie sprzętu i oprogramowania,
- rekomendacje łączące bezpieczeństwo, efektywność energetyczną i zasobową.

12:30–13:30 – Przerwa

13:30–14:15 – Współpraca zespołowa i zielona transformacja cyfrowa organizacji

Forma: praktyka

PRT: 4.2 Technologie informacyjne, 4.6 Bezpieczeństwo informacji

- współpraca przy wdrażaniu bezpiecznych i zasobooszczędnych rozwiązań IT,
- komunikowanie znaczenia efektywnego wykorzystania zasobów cyfrowych,
- łączenie wymogów bezpieczeństwa informacji z celami zielonej transformacji,
- konsultowanie decyzji technicznych dotyczących wykorzystania zasobów IT,
- rozwiązywanie sytuacji konfliktowych między wymaganiami bezpieczeństwa a celami środowiskowymi i wypracowywanie kompromisów.

14:15–16:00 – Walidacja efektów uczenia się / egzamin certyfikujący

Forma: walidacja

- test teoretyczny,
- obserwacja w warunkach symulowanych,

Harmonogram

Liczba pozycji harmonogramu: 12

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 12 Zielone cyberbezpieczeństwo i rodzaje zagrożeń cyfrowych	Zajęcia	Grzegorz Piwowarczyk	10-10-2026	09:00	10:30	01:30
2 z 12 Regulacje prawne, bezpieczeństwo informacji i odpowiedzialność cyfrowa	Zajęcia	Grzegorz Piwowarczyk	10-10-2026	10:30	12:00	01:30
3 z 12 Monitorowanie infrastruktury IT, analiza logów i optymalizacja zasobów cyfrowych	Zajęcia	Grzegorz Piwowarczyk	10-10-2026	12:00	13:00	01:00
4 z 12 -	Przerwa	-	10-10-2026	13:00	14:00	01:00
5 z 12 Energooszczędna infrastruktura IT i zrównoważone technologie cyfrowe	Zajęcia	Grzegorz Piwowarczyk	10-10-2026	14:00	15:30	01:30
6 z 12 Warsztaty praktyczne z zakresu zielonego cyberbezpieczeństwa	Zajęcia	Grzegorz Piwowarczyk	10-10-2026	15:30	17:00	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
7 z 12 Zarządzanie cyklem życia oprogramowania i ograniczanie e-odpadów	Zajęcia	Grzegorz Piwowarczyk	11-10-2026	08:00	09:30	01:30
8 z 12 Ekologiczna archiwizacja danych i optymalizacja zasobów cyfrowych	Zajęcia	Grzegorz Piwowarczyk	11-10-2026	09:30	10:30	01:00
9 z 12 Warsztaty praktyczne – organizacja procesów zielonego cyberbezpieczeństwa	Zajęcia	Grzegorz Piwowarczyk	11-10-2026	10:30	12:30	02:00
10 z 12 -	Przerwa	-	11-10-2026	12:30	13:30	01:00
11 z 12 Współpraca zespołowa i zielona transformacja cyfrowa organizacji	Zajęcia	Grzegorz Piwowarczyk	11-10-2026	13:30	14:15	00:45
12 z 12 -	Walidacja	-	11-10-2026	14:15	16:00	01:45

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	16:00
w tym suma godzin zajęć	12:15
w tym suma godzin walidacji	01:45
w tym suma przerw	02:00
Suma godzin dydaktycznych bez przerw	18:30

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	5 739,18 PLN
Koszt przypadający na 1 uczestnika netto	4 666,00 PLN
Koszt osobogodziny brutto	358,70 PLN
Koszt osobogodziny netto	291,63 PLN
W tym koszt walidacji brutto	492,00 PLN
W tym koszt walidacji netto	400,00 PLN
W tym koszt certyfikowania brutto	123,00 PLN
W tym koszt certyfikowania netto	100,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	16:00

Prowadzący

Liczba prowadzących: 1

1 z 1

Grzegorz Piwowarczyk

Trener z wieloletnim doświadczeniem zawodowym i szkoleniowym w branży IT, cyberbezpieczeństwa oraz nowoczesnych technologii cyfrowych. W latach 2021-2026 - rozwijał kompetencje w zakresie cyberbezpieczeństwa oraz zrównoważonego wykorzystania technologii IT, m.in. poprzez udział w szkoleniu „Zielone cyberbezpieczeństwo – bezpieczeństwo informacji i efektywne wykorzystanie zasobów IT", obejmującym zagadnienia efektywności energetycznej infrastruktury IT, ograniczania obciążenia systemów, zarządzania cyklem życia sprzętu i oprogramowania oraz redukcji e-odpadów. W praktyce zawodowej wykorzystywał tę wiedzę przy administrowaniu i optymalizacji systemów IT, zarządzaniu zasobami cyfrowymi, bezpieczeństwem informacji oraz rozwiązaniami wspierającymi ograniczenie zbędnego wykorzystania infrastruktury i wydłużanie jej cyklu życia. Posiada doświadczenie szkoleniowe zdobyte m.in. podczas realizacji usług rozwojowych w BUR, warsztatów ICT, szkoleń komputerowych oraz projektów współfinansowanych ze środków Unii Europejskiej, w tym: szkoleń „MS Excel i podstawy dostępności cyfrowej", szkoleń ICT dla uczestników projektów społecznych i unijnych, szkoleń w projekcie „Sztuczna Inteligencja Realne Wsparcie", szkoleń realizowanych w ramach KPO „Kompetencje cyfrowe dla nowoczesnej administracji publicznej

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały przekazywane w trakcie realizacji usługi:

- laptopy udostępnione na czas trwania szkolenia. (udostępnione na czas trwania usługi).
- prezentacja szkoleniowa w formie wyświetlanej. (slajdy),
- notatnik i długopis.

Materiały przekazywane po zakończeniu usługi:

- prezentacja szkoleniowa w formie elektronicznej.
- zestaw materiałów uzupełniających w formie elektronicznej (linki, checklisty, rekomendacje dobrych praktyk).

Informacje dodatkowe

Dostępność: Zapewniamy równy dostęp do usługi. Na zgłoszenie uczestnika uzgadniamy **równoważne formy** materiałów (np. większa czcionka, alternatywny sposób prezentacji)

Kontakt: **Koordynator ds. dostępności – Magdalena Kudzia, m.kudzia@change.info.pl, 574 454 645** (potwierdzenie do 2 dni roboczych).

Podstawa zwolnienia z VAT:

Zwolnienie na podstawie § 3 ust. 1 pkt 14 Rozporządzenia Ministra Finansów w sprawie zwolnień od podatku od towarów i usług, w przypadku usług kształcenia zawodowego lub przekwalifikowania zawodowego finansowanych w co najmniej 70% ze środków publicznych

Informacja dotycząca realizacji usługi zgodnie z wytycznymi:

Usługa rozwojowa realizowana w formie usługi stacjonarnej, zostanie zrealizowana zgodnie

z aktualnie obowiązującymi przepisami prawa i zaleceniami Ministerstwa Zdrowia i Głównego Inspektoratu Sanitarnego.

Adres

al. Księdza Biskupa Juliusza Bursche 3/-
43-460 Wisła

woj. śląskie

Hotel Gołębiewski - sala szkoleniowa

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja

Kontakt

Dagmara Podhorodecka

E-mail d.podhorodecka@change.info.pl
Telefon (+48) 530 800 606