Możliwość dofinansowania

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

Numer usługi 2026/05/07/51191/3545407

4 900,00 PLN brutto
4 900,00 PLN netto
306,25 PLN brutto/h
306,25 PLN netto/h
261,33 PLN cena rynkowa

NEXTDAY spółka z ograniczoną odpowiedzialnością

4,8 / 5

2 963 oceny

Wisła
Usługa szkoleniowa
stacjonarna
Zajęcia grupowe
16:00 h
25.07.2026 do 05.08.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Usługa skierowana jest do dorosłych uczestników rynku pracy, w szczególności: • osoby chcące zdobyć kompetencje w zakresie cyberbezpieczeństwa i ochrony danych • osoby odpowiedzialne za bezpieczeństwo informacji w firmach i instytucjach • właściciele i pracownicy MŚP wdrażający rozwiązania cyfrowe • 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 Do udziału w szkoleniu nie jest wymagane wcześniejsze doświadczenie ani wykształcenie kierunkowe.
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	24-07-2026
Forma prowadzenia usługi	stacjonarna
Podstawa uzyskania wpisu do BUR	Standard Usług Szkoleniowo– Rozwojowych PIFS SUS 3.0

Cel

Cel edukacyjny

Usługa przygotowuje uczestników do identyfikowania zagrożeń cyberbezpieczeństwa, ochrony danych oraz wdrażania bezpiecznych i energooszczędnych rozwiązań IT zgodnie z zasadami zrównoważonego rozwoju. Uczestnik rozwija umiejętności monitorowania infrastruktury sieciowej, organizacji procesów bezpieczeństwa informacji oraz zarządzania cyklem życia oprogramowania z uwzględnieniem redukcji zużycia energii i e-odpadów. Usługa kończy się egzaminem oraz uzyskaniem kwalifikacji.

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 uwzględnieniem zasad efektywności energetycznej	Przygotowuje rozwiązanie monitorowania ruchu sieciowego minimalizujące zużycie energii	Analiza dowodów i deklaracji
	Dokumentuje proces konfiguracji systemu z analizą redukcji obciążenia infrastruktury	Analiza dowodów i deklaracji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Organizuje szkolenia pracowników dotyczące bezpiecznego postępowania z danymi i cyberatakami	Przygotowuje materiały szkoleniowe w formatach cyfrowych minimalizujących papier	Analiza dowodów i deklaracji
	Planuje szkolenia zdalne z wykorzystaniem platform e-learningowych i modułów interaktywnych	Analiza dowodów i deklaracji
Przeprowadza audyty archiwów logów bezpieczeństwa i wdraża procesy archiwizacji z kompresją	Analizuje istniejące systemy przechowywania logów i identyfikuje możliwości optymalizacji	Analiza dowodów i deklaracji
	Opracowuje procedury archiwizacji danych zgodnie z wymogami prawnymi i efektywnością zasobów	Analiza dowodów i deklaracji
Zarządza cyklem życia oprogramowania wspierając open-source i długoterminowe wsparcie	Planuje strategię aktualizacji oprogramowania, minimalizującą niepotrzebne zmiany sprzętu	Analiza dowodów i deklaracji
	Dokumentuje proces oceny oprogramowania open-source w kontekście bezpieczeństwa i ekologii	Analiza dowodów i deklaracji
Promuje zasady etyki zawodowej i odpowiedzialności zasobowej w komunikacji z zespołem IT	Demonstruje świadome podejście do zasobów poprzez wspieranie inicjatyw zielonego cyberbezpieczeństwa	Analiza dowodów i deklaracji
	Komunikuje znaczenie zrównoważonego rozwoju w kontekście działań bezpieczeństwa informacji	Analiza dowodów i deklaracji
Współpracuje interdyscyplinarnie z działami IT, kadrami i kadrą zarządzającą w celu realizacji celów ekologicznych	Koordynuje projekty bezpieczeństwa z uwzględnieniem wymogów zrównoważonego rozwoju	Analiza dowodów i deklaracji
	Konsultuje decyzje techniczne z pracownikami różnych departamentów w sprawie zasobów	Analiza dowodów i deklaracji
Ocenia skuteczność działań bezpieczeństwa pod względem zarówno ochrony, jak i efektywności	Analizuje metryki bezpieczeństwa i wskaźniki zużycia energii w procesach ochrony danych	Analiza dowodów i deklaracji
	Rekomenduje działania usprawniające opierające się na zbalansowaniu bezpieczeństwa i ekologii	Analiza dowodów i deklaracji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Doskonali umiejętności rozwiązywania konfliktów między wymogami bezpieczeństwa a zielonymi celami	Opracowuje strategie negocjacji w przypadku sprzeczności między ochroną danych a efektywnością	Analiza dowodów i deklaracji
	Znajduje kompromisowe rozwiązania łączące wysokie standardy bezpieczeństwa z praktykami ekologicznymi	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://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

Grupa docelowa: Szkolenie skierowane jest do grup:

- osoby chcące zdobyć kompetencje w zakresie cyberbezpieczeństwa i ochrony danych
- osoby odpowiedzialne za bezpieczeństwo informacji w firmach i instytucjach
- właściciele i pracownicy MŚP wdrażający rozwiązania cyfrowe
- 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

Kwalifikacje:

Usługa prowadzi do uzyskania kwalifikacji SPECJALISTA DS. CYBERBEZPIECZEŃSTWA (Cybersecurity Specialist, GCCS-DIG-004, Category G – Green) nadawanej przez międzynarodowy podmiot certyfikujący.

Egzamin kwalifikacyjny ma formę testu teoretycznego oraz analizy dowodów i deklaracji i przeprowadzany jest zgodnie ze standardami GCCS przez niezależny podmiot walidujący.

Proces walidacji efektów uczenia się w trakcie usługi prowadzony jest przez podmiot zewnętrzny – ICVC Certyfikacja Sp. z o.o. – i obejmuje weryfikację osiągnięcia efektów uczenia się na podstawie zdefiniowanych kryteriów

Sposób Walidacji i egzamin

test teoretyczny

analiza dowodów i deklaracji

Czas oczekiwania na wynik walidacji oraz na dokument wystawiany przez uprawniony podmiot certyfikujący potwierdzający nadanie określonej kwalifikacji w przypadku pozytywnego wyniku przeprowadzonej walidacji wynosi do 8 dni roboczych od dnia egzaminu.

Realizacja szkolenia: 25-26.07. 2026 r.

Oczekiwanie na wynik walidacji oraz dokumentu - do 5.08.2026 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 Programem Rozwoju Technologii Województwa Śląskiego 2019–2030

Usługa jest powiązana z Programem Rozwoju Technologii Województwa Śląskiego 2019–2030 w obszarze technologicznym:

1. 1. Technologie informacyjne i telekomunikacyjne
    - 4.2 Technologie informacyjne
    - 4.6 Bezpieczeństwo informacji

Powiązanie wynika z rozwijania kompetencji w zakresie cyberbezpieczeństwa, ochrony danych, monitorowania infrastruktury IT oraz wdrażania energooszczędnych i zrównoważonych rozwiązań cyfrowych.

Warunki organizacyjne:

- usługa realizowana jest w formie warsztatowej, z przewagą zajęć praktycznych 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,

Usługa realizowana jest w godzinach zegarowych.

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

PROGRAM USŁUGI

PROGRAM USŁUGI

DZIEŃ I – 9:00–17:00

(4h teoria / 3h praktyka / 1h przerwa)

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

Forma: teoria

- rodzaje zagrożeń cyberbezpieczeństwa
- phishing, malware, ransomware, ataki socjotechniczne
- identyfikacja zagrożeń w systemach IT
- bezpieczeństwo danych i użytkowników
- wpływ cyberzagrożeń na ciągłość i efektywność organizacji

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

Forma: teoria

- RODO i ochrona danych osobowych
- standardy i normy bezpieczeństwa informacji
- odpowiedzialność organizacji za bezpieczeństwo danych
- etyka zawodowa i odpowiedzialność zasobowa
- cyfrowy obieg informacji i ograniczanie dokumentacji papierowej

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

Forma: praktyka

- analiza ruchu sieciowego
- identyfikacja nieprawidłowości i zagrożeń
- monitorowanie obciążenia infrastruktury IT
- optymalizacja wykorzystania zasobów cyfrowych
- dokumentowanie incydentów bezpieczeństwa

13:00–14:00 – Przerwa

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

Forma: teoria

- wpływ infrastruktury IT na zużycie energii i emisję CO_2
- energooszczędne rozwiązania w cyberbezpieczeństwie
- ograniczanie e-odpadów i wydłużanie cyklu życia sprzętu
- open-source i zrównoważony rozwój w IT
- ograniczanie śladu cyfrowego organizacji

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

Forma: praktyka

- konfiguracja narzędzi monitorowania infrastruktury IT
- analiza logów bezpieczeństwa
- organizacja bezpiecznego i energooszczędnego środowiska pracy
- opracowanie działań ograniczających obciążenie infrastruktury IT
- optymalizacja wykorzystania zasobów cyfrowych

DZIEŃ II – 8:00–16:00

(3,5h teoria / 2,5h praktyka / 1h przerwa / 1h walidacja)

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

Forma: teoria

- aktualizacje systemów i bezpieczeństwo
- planowanie infrastruktury IT zgodnie z zasadami efektywności zasobowej
- ograniczanie nadmiernej wymiany sprzętu
- znaczenie długoterminowego wsparcia oprogramowania
- open-source jako element zrównoważonego rozwoju

09:30–11:00 – Ekologiczna archiwizacja danych i optymalizacja zasobów cyfrowych

Forma: teoria

- przechowywanie i kompresja logów
- procedury archiwizacji danych
- ograniczanie nadmiarowego przechowywania danych
- efektywne wykorzystanie przestrzeni dyskowej
- bezpieczeństwo i retencja danych

11:00–13:00 – Warsztaty praktyczne – organizacja procesów zielonego cyberbezpieczeństwa

Forma: praktyka

- przygotowanie procedur bezpieczeństwa
- planowanie szkoleń cyfrowych dla pracowników
- tworzenie materiałów elektronicznych ograniczających zużycie papieru
- analiza efektywności energetycznej działań bezpieczeństwa
- opracowanie rekomendacji dla organizacji

13:00–14:00 – Przerwa

14:00–15:00 – Współpraca zespołowa i zielona transformacja cyfrowa organizacji

Forma: praktyka

- komunikacja z zespołami IT i kadrą zarządzającą
- rozwiązywanie konfliktów między bezpieczeństwem a efektywnością energetyczną
- wdrażanie zasad zrównoważonego rozwoju w środowisku IT
- planowanie działań wspierających zieloną transformację cyfrową

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

Forma: walidacja

- test teoretyczny
- analiza dowodów i deklaracji

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	25-07-2026	09:00	10:30	01:30
2 z 12 Regulacje prawne, bezpieczeństwo informacji i odpowiedzialność cyfrowa	Zajęcia	Grzegorz Piwowarczyk	25-07-2026	10:30	12:00	01:30
3 z 12 Monitorowanie infrastruktury IT, analiza logów i optymalizacja zasobów cyfrowych	Zajęcia	Grzegorz Piwowarczyk	25-07-2026	12:00	13:00	01:00
4 z 12 -	Przerwa	-	25-07-2026	13:00	14:00	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 12 Energooszczędna infrastruktura IT i zrównoważone technologie cyfrowe	Zajęcia	Grzegorz Piwowarczyk	25-07-2026	14:00	15:30	01:30
6 z 12 Warsztaty praktyczne z zakresu zielonego cyberbezpieczeństwa	Zajęcia	Grzegorz Piwowarczyk	25-07-2026	15:30	17:00	01:30
7 z 12 Zarządzanie cyklem życia oprogramowania i ograniczanie e-odpadów	Zajęcia	Grzegorz Piwowarczyk	26-07-2026	08:00	09:30	01:30
8 z 12 Ekologiczna archiwizacja danych i optymalizacja zasobów cyfrowych	Zajęcia	Grzegorz Piwowarczyk	26-07-2026	09:30	11:00	01:30
9 z 12 Warsztaty praktyczne – organizacja procesów zielonego cyberbezpieczeństwa	Zajęcia	Grzegorz Piwowarczyk	26-07-2026	11:00	13:00	02:00
10 z 12 -	Przerwa	-	26-07-2026	13:00	14:00	01:00
11 z 12 Współpraca zespołowa i zielona transformacja cyfrowa organizacji	Zajęcia	Grzegorz Piwowarczyk	26-07-2026	14:00	15:00	01:00
12 z 12 -	Walidacja	-	26-07-2026	15:00	16:00	01:00

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	16:00
w tym suma godzin zajęć	13:00
w tym suma godzin walidacji	01:00
w tym suma przerw	02:00
Suma godzin dydaktycznych bez przerw	18:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 900,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	4 900,00 PLN
Koszt osobogodziny brutto	306,25 PLN
Koszt osobogodziny netto	306,25 PLN
W tym koszt walidacji brutto	400,00 PLN
W tym koszt walidacji netto	400,00 PLN
W tym koszt certyfikowania brutto	100,00 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 ciągu ostatnich 5 lat realizował szkolenia i warsztaty z zakresu kompetencji cyfrowych, obsługi systemów informatycznych, bezpieczeństwa IT, infrastruktury sieciowej oraz nowoczesnych narzędzi technologicznych, z uwzględnieniem zasad efektywności energetycznej, bezpieczeństwa danych oraz zrównoważonego wykorzystania zasobów cyfrowych.
Od 2022 roku prowadzi własną działalność gospodarczą w branży IT, realizując usługi związane z administracją systemów, bezpieczeństwem IT, sieciami komputerowymi, bazami danych, wdrażaniem i optymalizacją systemów informatycznych oraz szkoleniami z zakresu kompetencji cyfrowych i technologicznych. Specjalizuje się m.in. w systemach operacyjnych Microsoft, Active Directory, rozwiązaniach chmurowych, bezpieczeństwie IT oraz optymalizacji infrastruktury informatycznej, wspierającej ograniczanie zużycia energii i efektywne zarządzanie zasobami IT.
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).

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