Możliwość dofinansowania

Szkolenie: Cyberhigiena i bezpieczeństwo cyfrowe w sytuacjach kryzysowych. Szkolenie z egzaminem kwalifikacyjnym.

Numer usługi 2025/11/12/145810/3142869

5 000,00 PLN brutto
5 000,00 PLN netto
294,12 PLN brutto/h
294,12 PLN netto/h

Martess MARLENA GRZYMKIEWICZ

★★★★★ 5,0 / 5

607 ocen

Bytom / stacjonarna
Usługa szkoleniowa
17 h
31.01.2026 do 01.02.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	**Grupa Docelowa:** Szkolenie jest dedykowane szerokiej grupie odbiorców, którzy na co dzień korzystają z technologii cyfrowych, a w szczególności: • **Pracownikom mikro, małych i średnich przedsiębiorstw (MŚP)**, którzy w swojej pracy przetwarzają dane osobowe, korzystają z systemów firmowych, lub są odpowiedzialni za kluczowe procesy, a jednocześnie nie są specjalistami IT. • **Osobom indywidualnym i pracownikom administracji publicznej**, którzy chcą podnieść swoją odporność cyfrową i umiejętności obronne przed zagrożeniami w cyberprzestrzeni, w tym w kontekście dezinformacji i ochrony danych osobowych (RODO). • **Wszystkim pełnoletnim obywatelom** zainteresowanym proaktywną ochroną swojej prywatności i danych w sytuacjach podwyższonego ryzyka cyfrowego lub kryzysowego.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	26-01-2026
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	17
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

Po szkoleniu uczestnicy będą zdolni do samodzielnego implementowania protokołów cyberhigieny oraz technik szyfrowania i anonimizacji w celu ochrony krytycznych zasobów informacyjnych i komunikacji w warunkach podwyższonego zagrożenia, takich jak kryzys militarny, klęska żywiołowa lub blackout. Ponadto, usługa umożliwia skuteczne rozpoznawanie dezinformacji i działań socjotechnicznych oraz planowanie awaryjnej komunikacji i cyfrowego planu przetrwania.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje kluczowe zasady cyberhigieny i bezpiecznej komunikacji w warunkach kryzysu (np. brak sieci, blackout).	Uczestnik wyjaśnia hierarchię priorytetów ochrony danych oraz wskazać protokoły awaryjnej komunikacji (szyfrowanie, VPN).	Test teoretyczny
Definiuje zagrożenia asymetryczne i identyfikuje mechanizmy dezinformacji oraz ataków socjotechnicznych (phishing, vishing).	Uczestnik poprawnie rozróżnia typy zagrożeń i podaje strategie weryfikacji źródeł (fact-checking) w warunkach podwyższonego ryzyka.	Test teoretyczny
Wdraża plan awaryjny w zakresie cyfrowej ciągłości działania i zarządzania zasobami informacyjnymi (np. procedury offline access, backup zaszyfrowanych danych).	Uczestnik wskazuje niezbędne etapy tworzenia i utrzymania zaszyfrowanych kopii zapasowych (backup) oraz określa procedury odzyskiwania danych.	Test teoretyczny
Analizuje ryzyko utraty danych i optymalizuje ustawienia zabezpieczeń w kluczowych aplikacjach (np. menedżery haseł, uwierzytelnianie dwuskładnikowe).	Uczestnik ocenia poziom ryzyka poszczególnych kont oraz wskazać najlepsze praktyki w zakresie twardych haseł i ich rotacji.	Test teoretyczny
Określa kluczowe zasady First Aid (pierwszej pomocy) i planuje zawartość plecaka ucieczkowego (BOB) w kontekście utrzymania sprzętu komunikacyjnego w gotowości (np. ładowarki solarne, powerbanki).	Uczestnik opisuje zawartość zestawu pierwszej pomocy i uzasadnia wybór źródeł zasilania awaryjnego dla urządzeń cyfrowych.	Test teoretyczny
Podejmuje odpowiedzialność za bezpieczeństwo informacji, działając zgodnie z normami społecznymi i etyką w sytuacjach kryzysowych (Kompetencja Społeczna).	Uczestnik uzasadnia konieczność zachowania dyskrecji, cierpliwości i uprzejmości (np. w komunikacji kryzysowej) oraz zna zasady etyki w ochronie danych.	Test teoretyczny
Organizuje bezpieczne środowisko pracy/domowe poprzez wdrażanie zasad kontroli dostępu fizycznego i cyfrowego.	Uczestnik opisuje różnice między kontrolą dostępu fizycznego a logicznego i wskazuje środki zabezpieczeń adekwatne do danego środowiska.	Test teoretyczny

Kwalifikacje

Inne kwalifikacje

Uznane kwalifikacje

Pytanie 4. Czy dokument potwierdzający uzyskanie kwalifikacji jest rozpoznawalny i uznawalny w danej branży/sektorze (czy certyfikat otrzymał pozytywne rekomendacje od co najmniej 5 pracodawców danej branży/ sektorów lub związku branżowego, zrzeszającego pracodawców danej branży/sektorów)?

TAK

Informacje

Podstawa prawna dla Podmiotów / kategorii Podmiotów	uprawnionych do wydawania dokumentów potwierdzających uzyskanie kwalifikacji, w tym w zawodzie
Nazwa Podmiotu prowadzącego walidację	FUNDACJA MY PERSONALITY SKILLS
Podmiot prowadzący walidację jest zarejestrowany w BUR	Tak
Nazwa Podmiotu certyfikującego	FUNDACJA MY PERSONALITY SKILLS
Podmiot certyfikujący jest zarejestrowany w BUR	Tak

Program

Aby został zrealizowany główny cel usługi kursant powinien:

- **Posiadać podstawową umiejętność obsługi komputera** i przeglądarki internetowej, co jest niezbędne do wdrożenia protokołów cyberhigieny.
- **Umieć obsługiwać edytor tekstu i arkusz kalkulacyjny** (np. MS Office / Google Workspace) w stopniu umożliwiającym tworzenie notatek, zaszyfrowanych planów awaryjnych oraz proste wprowadzanie danych do gotowych tabel (nie jest wymagana zaawansowana znajomość).
- **Wykazywać silną motywację do rozwoju osobistego** oraz **zdobycia przyszłościowych kompetencji zarządczych i obronnych**, kluczowych w warunkach podwyższonego ryzyka.
- **Być gotowym do aktywnego uczestnictwa w warsztatach, dyskusjach i pracy grupowej**, co jest fundamentem w rozwoju kompetencji społecznych niezbędnych do zarządzania informacją w kryzysie.

Szkolenie zostało zaprojektowane zgodnie z założeniami **Programu Rozwoju Technologii (PRT) Województwa Śląskiego** i **Funduszu Sprawiedliwej Transformacji (FST)**, stanowiąc strategiczne rozwinięcie kompetencji z obszarów:

- **Zielonej Transformacji (PRT-3):** Szkolenie bezpośrednio realizuje cele dekarbonizacji i **zarządzania zasobami**, przenosząc je na poziom **gotowości kryzysowej**. Uczy, jak **optymalizować zużycie energii i zasobów** (Zielone Kompetencje) oraz planować autonomię w warunkach braku infrastruktury (np. blackout) – co jest kluczowe dla **ciągłości działania (BCP)**.
- **Technologie ICT (PRT-4):** Usługa koncentruje się na **technologiach ICT wspierających zarządzanie bezpieczeństwem i informacją**. Wymogi obronne wymuszają cyfryzację procesów ochrony i szyfrowania. Moduły dotyczące ochrony przed dezinformacją i planowania awaryjnej komunikacji rozwijają kompetencje z zakresu **zarządzania krytycznymi zbiorami danych** (Data Gaps Analysis) i wykorzystania systemów IT/szyfrowania do **utrzymania bezpieczeństwa (PRT-4.7)**.

PROGRAM SZKOLENIA:

Moduł 1: Podstawy ryzyka kryzysowego i cyfrowej gotowości

- Wprowadzenie do zarządzania ryzykiem cyfrowym w skrajnych scenariuszach (m.in. blackout, konflikt).
- Analiza celów ataku na jednostkę i firmę w kontekście gotowości obronnej.
- Wdrażanie koncepcji **Cyfrowego Plecaka Ucieczkowego (BOB)** i strategii "zero zaufania".

Moduł 2: Zaawansowana cyberhigiena awaryjna

- Praktyczne wdrażanie protokołów bezpieczeństwa w warunkach odcięcia od sieci.
- Zasady twardych haseł w kryzysie, rotacja i zarządzanie nimi za pomocą menedżerów haseł.
- Charakteryzowanie i wdrażanie uwierzytelniania wieloskładnikowego (MFA) poza tradycyjnymi sieciami.

Moduł 3: Zarządzanie informacją i komunikacja awaryjna

- Analiza prawnych i etycznych aspektów **szyfrowania** (RODO, tajemnica korespondencji) w sytuacji zagrożenia.
- Wdrażanie bezpiecznych, zaszyfrowanych kanałów komunikacji i planów komunikacji **offline**.

Moduł 4: Dezinformacja, propaganda i inżynieria społeczna

- Definiowanie mechanizmów **propagandy i dezinformacji** w konflikcie.
- Techniki **fact-checkingu** w warunkach braku mediów i chaosu informacyjnego.
- Organizacja bezpiecznego środowiska informacyjnego i unikanie rozprzestrzeniania fake news.

Moduł 5: Cyfrowy plan przetrwania (Backup i Recovery)

- Wdrażanie łańcucha **bezpiecznego backupu** (zasada 3-2-1) dla krytycznych zasobów.
- Charakteryzowanie typów szyfrowania dla kopii zapasowych i analiza zagrożenia *ransomware*.

Moduł 6: Identyfikacja i reagowanie na incydenty

- Definiowanie różnicy między atakiem a incydentem bezpieczeństwa.
- Planowanie procedur postępowania po włamaniu na konto firmowe/prywatne.
- Organizowanie awaryjnego odzyskiwania dostępu i danych.

Moduł 7: Bezpieczeństwo urządzeń i infrastruktury

- Analiza słabych punktów urządzeń mobilnych (telefony, laptopy) i ich zabezpieczanie.
- Określanie zasad bezpiecznego korzystania z publicznych sieci i ładowania awaryjnego (np. powerbanki, ładowarki solarne).
- Wdrażanie zasad kontroli dostępu fizycznego i cyfrowego do sprzętu.

Moduł 8 WALIDACJA

Szkolenie realizowanie w godzinach zegarowych, przerwy wliczają się w czas trwania usługi.

Harmonogram

Liczba przedmiotów/zajęć: 13

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 13 Moduł 1: Podstawy ryzyka kryzysowego i cyfrowej gotowości	Konstancja Iwanek	31-01-2026	09:00	10:45	01:45
2 z 13 Przerwa	Konstancja Iwanek	31-01-2026	10:45	11:00	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
3 z 13 Moduł 2: Zaawansowana cyberhigiena awaryjna	Konstancja Iwanek	31-01-2026	11:00	13:45	02:45
4 z 13 Przerwa	Konstancja Iwanek	31-01-2026	13:45	14:00	00:15
5 z 13 Moduł 3: Zarządzanie informacją i komunikacja awaryjna	Konstancja Iwanek	31-01-2026	14:00	15:45	01:45
6 z 13 Przerwa	Konstancja Iwanek	31-01-2026	15:45	16:00	00:15
7 z 13 Moduł 4: Dezinformacja, propaganda i inżynieria społeczna	Konstancja Iwanek	31-01-2026	16:00	18:30	02:30
8 z 13 Moduł 5: Cyfrowy plan przetrwania (Backup i Recovery)	Konstancja Iwanek	31-01-2026	18:30	20:00	01:30
9 z 13 Moduł 6: Identyfikacja i reagowanie na incydenty	Konstancja Iwanek	01-02-2026	09:00	11:15	02:15
10 z 13 Przerwa	Konstancja Iwanek	01-02-2026	11:15	11:30	00:15
11 z 13 Moduł 7: Bezpieczeństwo urządzeń i infrastruktury	Konstancja Iwanek	01-02-2026	11:30	13:45	02:15
12 z 13 Przerwa	Konstancja Iwanek	01-02-2026	13:45	14:00	00:15
13 z 13 Walidacja	-	01-02-2026	14:00	15:00	01:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 000,00 PLN
Koszt przypadający na 1 uczestnika netto	5 000,00 PLN
Koszt osobogodziny brutto	294,12 PLN
Koszt osobogodziny netto	294,12 PLN
W tym koszt walidacji brutto	300,00 PLN
W tym koszt walidacji netto	300,00 PLN
W tym koszt certyfikowania brutto	300,00 PLN
W tym koszt certyfikowania netto	300,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Konstancja Iwanek

Konstancja Iwanek jest specjalistką w obszarze nowych mediów, komunikacji cyfrowej i edukacji technologicznej. Absolwentka kierunku prawa na Uniwersytecie Śląskim. Aktywnie związana z projektami edukacyjnymi i szkoleniowymi w sektorze IT i edukacji cyfrowej, w tym jako trenerka kompetencji medialnych, doradczyni ds. transformacji cyfrowej. Jej doświadczenie obejmuje projektowanie i wdrażanie nowoczesnych rozwiązań edukacyjnych, zarządzanie procesami szkoleniowymi w organizacjach, a także prowadzenie szkoleń w zakresie minimalizmu technologicznego, zarządzania danymi i wdrażania zielonych kompetencji cyfrowych. Specjalizuje się w tematyce zrównoważonego zarządzania technologią, cyfrowego wellbeing oraz ograniczania tzw. „dark data" w organizacjach. W swojej praktyce łączy perspektywę technologiczną z humanistyczną, kładąc nacisk na odpowiedzialne i świadome korzystanie z narzędzi cyfrowych. Prowadziła liczne warsztaty z zakresu cyfrowej higieny, edukacji medialnej oraz cyfrowej transformacji w biznesie i edukacji, ze szczególnym uwzględnieniem aspektów środowiskowych. Doświadczenie zdobyte nie wcześniej niż 5 lat pięć lat. Aktywnie rozwija kompetencje trenerskie w zakresie cyfrowych technologii i ich wpływu na dobrostan oraz efektywność organizacyjną.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Warunki Uczestnictwa

- **Wymagania formalne:** Pełnoletność.
- **Wiedza i umiejętności:** Wymagana jest podstawowa umiejętność obsługi komputera i korzystania z Internetu. Nie jest wymagane specjalistyczne wykształcenie informatyczne.
- **Wymagania techniczne:** Uczestnik powinien posiadać własne urządzenie mobilne (smartfon/laptop) do pracy podczas warsztatów, co pozwoli na spersonalizowane wdrożenie poznanych protokołów bezpieczeństwa.

Dodatkowe Informacje o Usłudze

- **Materiały dla uczestników:** Uczestnicy otrzymają kompletny **skrypt szkoleniowy** (obejmujący teorię i protokoły postępowania awaryjnego), **długopis i notatnik** do sporządzania notatek oraz listę rekomendowanych narzędzi do bezpiecznej komunikacji i weryfikacji informacji.
- **Udogodnienia w miejscu realizacji:** W miejscu realizacji usługi zapewniona jest **Klimatyzacja** oraz dostęp do **Wi-Fi** (wykorzystywany do ćwiczeń na kontrolowanej sieci).
- **Zgodność z Funduszami (PRT/FST):** Szkolenie jest zaprojektowane zgodnie z założeniami **Funduszu Sprawiedliwej Transformacji (FST)** w obszarze rozwijania **zielonych kompetencji** i podnoszenia **odporności cyfrowej i społecznej**, co jest kluczowe dla ciągłości funkcjonowania przedsiębiorstw i regionów w warunkach kryzysu (Obszar PRT 3).

Informacje dodatkowe

Walidacja i certyfikacja przebiega pod nadzorem komisji walidacyjnej, która składa się z osób nieuczestniczących w procesie szkoleniowym i spełniających kryteria kwalifikacyjne określone w Zintegrowanym Systemie Kwalifikacji (ZSK).

Usługa realizowana w formie usługi stacjonarnej zostanie w całości zrealizowana zgodnie z aktualnie obowiązującymi przepisami prawa i zaleceniami Ministerstwa Zdrowia i Głównego Inspektoratu Sanitarnego.

Podstawy prawne zwolnienia z vat : 1. Rozporządzenie Ministra Finansów z dn. 20.12.2013 r. paragraf 3 ust 1 pkt.14. Zwalnia się od podatku usługi kształcenia zawodowego lub przekwalifikowania zawodowego , finansowane w co najmniej 70 % ze środków publicznych oraz świadczenie usług i dostawę towarów ściśle z tymi usługami związane.

Adres

ul. Wojciecha Korfantego 21

41-902 Bytom

woj. śląskie

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi

Kontakt

Karolina Myszka

E-mail myszkakarolinaa@gmail.com

Telefon (+48) 798 645 481