Możliwość dofinansowania

Martess MARLENA GRZYMKIEWICZ

5,0 / 5

680 ocen

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

Numer usługi 2026/06/02/145810/3603143

Bytom
Usługa szkoleniowa
stacjonarna
Zajęcia grupowe
16:00 h
29.07.2026 do 30.07.2026

4 600,00 PLN brutto
4 600,00 PLN netto
287,50 PLN brutto/h
287,50 PLN netto/h
261,33 PLN cena rynkowa

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	5
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	28-07-2026
Forma prowadzenia usługi	stacjonarna
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

Szkolenie przygotowuje uczestnika do nabycia kwalifikacji oraz 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 wskazuje hierarchię priorytetów ochrony danych oraz 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 wskazuje 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 wskazuje 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.	Uczestnik charakteryzuje 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 charakteryzuje różnice między kontrolą dostępu fizycznego a logicznego i wskazuje środki zabezpieczeń adekwatne do danego środowiska.	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://my-ps.eu/ , https://my-ps.eu/dzialalnosc-miedzynarodowa/

Informacje

Nazwa Podmiotu prowadzącego walidację	FUNDACJA MY PERSONALITY SKILLS
Nazwa Podmiotu certyfikującego	FUNDACJA MY PERSONALITY SKILLS

Program

Szkolenie zostało zaprojektowane zgodnie z założeniami **REGIONALNEJ STRATEGII INNOWACJI WOJEWÓDZTWA ŚLĄSKIEGO oraz 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)**.

Zajęcia teoretycznie: 6,15 godzin

Zajęcia praktyczne: 7 godzin

Przerwy: 2 godziny

Walidacja: 0,45 godzin

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".

Kompetencje rozwijane w module: Zielone kompetencje, cyfrowe kompetencje, realizacja PRT 3

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.

Kompetencje rozwijane w module: Cyfrowe kompetencje, realizacja PRT 4

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.

Kompetencje rozwijane w module: Cyfrowe kompetencje

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*.

Kompetencje rozwijane w module: Zielone kompetencje, cyfrowe kompetencje, realizacja PRT 4

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.

Kompetencje rozwijane w module: Cyfrowe kompetencje, realizacja PRT 3

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.

Kompetencje rozwijane w module: Zielone kompetencje, cyfrowe kompetencje, realizacja PRT 3, PRT 4

Moduł 8 WALIDACJA

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

Harmonogram

Liczba pozycji harmonogramu: 14

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 14 Moduł 1: Podstawy ryzyka kryzysowego i cyfrowej gotowości	Zajęcia	Konstancja Iwanek	29-07-2026	09:00	10:45	01:45
2 z 14 -	Przerwa	-	29-07-2026	10:45	11:00	00:15
3 z 14 Moduł 2: Zaawansowana cyberhigiena awaryjna	Zajęcia	Konstancja Iwanek	29-07-2026	11:00	13:45	02:45

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
4 z 14 -	Przerwa	-	29-07-2026	13:45	14:15	00:30
5 z 14 Moduł 3: Zarządzanie informacją i komunikacja awaryjna	Zajęcia	Konstancja Iwanek	29-07-2026	14:15	15:45	01:30
6 z 14 -	Przerwa	-	29-07-2026	15:45	16:00	00:15
7 z 14 Moduł 4: Dezinformacja, propaganda i inżynieria społeczna	Zajęcia	Konstancja Iwanek	29-07-2026	16:00	17:00	01:00
8 z 14 Moduł 5: Cyfrowy plan przetrwania (Backup i Recovery)	Zajęcia	Konstancja Iwanek	30-07-2026	09:00	10:45	01:45
9 z 14 -	Przerwa	-	30-07-2026	10:45	11:00	00:15
10 z 14 Moduł 6: Identyfikacja i reagowanie na incydenty	Zajęcia	Konstancja Iwanek	30-07-2026	11:00	13:15	02:15
11 z 14 -	Przerwa	-	30-07-2026	13:15	13:30	00:15
12 z 14 Moduł 7: Bezpieczeństwo urządzeń i infrastruktury	Zajęcia	Konstancja Iwanek	30-07-2026	13:30	15:45	02:15
13 z 14 -	Przerwa	-	30-07-2026	15:45	16:15	00:30
14 z 14 -	Walidacja	-	30-07-2026	16:15	17:00	00:45

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	16:00

Rodzaj godzin	Liczba godzin
w tym suma godzin zajęć	13:15
w tym suma godzin walidacji	00:45
w tym suma przerw	02:00
Suma godzin dydaktycznych bez przerw	18:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	4 600,00 PLN
Koszt przypadający na 1 uczestnika netto	4 600,00 PLN
Koszt osobogodziny brutto	287,50 PLN
Koszt osobogodziny netto	287,50 PLN
W tym koszt walidacji brutto	300,00 PLN
W tym koszt walidacji netto	300,00 PLN
W tym koszt certyfikowania brutto	600,00 PLN
W tym koszt certyfikowania netto	600,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	16:00

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

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.
- **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 **REGIONALNEJ STRATEGII INNOWACJI WOJEWÓDZTWA ŚLĄSKIEGO** oraz **Funduszu Sprawiedliwej Transformacji (FST)** w obszarze rozwijania **zielonych kompetencji** i podnoszenia **odporności cyfrowej i społeczne,** 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)**.

Informacje dodatkowe

Szkolenie realizowane jest w terminie 29-30.07.2026 r po jego zakończeniu uczestnicy przystępują do egzaminu certyfikującego organizowanego i ocenianego przez podmiot zewnętrzny. Ze względu na sposób przeprowadzenia walidacji wynik otrzymywany jest natychmiastowo po przeprowadzeniu walidacji. Osoba przeprowadzająca walidację zobowiązana jest do wystawienia wyników egzaminu w dniu zakończeniu szkolenia.

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. Martess Academy posiada wpis do Rejestru Niepublicznych Placówek Oświatowych, co stanowi podstawę zwolnienia z VAT w przypadku usług innych niż w/w.

Adres

ul. Wojciecha Korfantego 21

41-902 Bytom

woj. śląskie

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi

Kontakt

MARLENA GRZYMKIEWICZ

E-mail marlena@martess.pl

Telefon (+48) 503 674 215