Możliwość dofinansowania

Praktyczne cyberbezpieczeństwo: techniki ochrony danych i komunikacji w Internecie – Szkolenie zakończone kwalifikacją.

Numer usługi 2026/08/31/217047/3779440

5 200,00 PLN brutto
5 200,00 PLN netto
346,67 PLN brutto/h
346,67 PLN netto/h
261,33 PLN cena rynkowa

Future Skills Teresa Węglarz

Brak ocen dla tego dostawcy

- Mysłowice
- Usługa szkoleniowa
- stacjonarna
- Zajęcia grupowe
- 15:00 h
- 04.10.2026 do 25.10.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie przeznaczone dla osób indywidualnych, które chcą podnosić kwalifikacje z własnej inicjatywy. Pracownicy biurowi, którzy chcą wykorzystać je w obecnej lub przyszłej pracy zawodowej, w szczególności do osób planujących rozpoczęcie pracy w obszarze cyberbezpieczeństwa. Udział w szkoleniu nie wymaga wcześniejszego doświadczenia zawodowego w cyberbezpieczeństwie. Wymagana jest podstawowa umiejętność obsługi komputera, korzystania z Internetu, poczty elektronicznej oraz aplikacji biurowych. Szkolenie jest przeznaczone dla osób początkujących, które chcą zdobyć uporządkowane podstawy do dalszego rozwoju zawodowego w branży cyberbezpieczeństwa.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	5
Data zakończenia rekrutacji	30-09-2026
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

Przygotowanie uczestnika do zaawansowanego rozpoznawania zagrożeń cyfrowych oraz wdrażania procedur ochrony danych i komunikacji, przy uwzględnieniu zrównoważonego zarządzania infrastrukturą IT. Uczestnik nabędzie kompetencje w zakresie optymalizacji mocy obliczeniowej, ograniczania nadmiarowego przetwarzania informacji oraz budowania odporności cyfrowej, która wydłuża cykl życia urządzeń i redukuje powstawanie elektroodpadów. Przygotowuje do działań zgodnych z GreenComp.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wiedza: Charakteryzuje podstawowe zagrożenia cyberbezpieczeństwa w środowisku firmowym i indywidualnym oraz ich wpływ na ciągłość procesów cyfrowych i wykorzystanie zasobów IT.	rozróżnia phishing, złośliwe oprogramowanie, ataki na hasła i socjotechnikę;	Test teoretyczny z wynikiem generowanym automatycznie
	wskazuje skutki incydentu dla danych, urządzeń i ciągłości pracy;	Test teoretyczny z wynikiem generowanym automatycznie
	wskazuje sytuacje powodujące konieczność odtwarzania danych lub ponownego wykonywania pracy.	Test teoretyczny z wynikiem generowanym automatycznie
Wiedza: Rozróżnia podstawowe pojęcia i mechanizmy stosowane w cyberbezpieczeństwie oraz zasady bezpiecznego i efektywnego wykorzystania danych, urządzeń i komunikacji cyfrowej.	Identyfikuje co najmniej trzy sytuacje, w których incydenty i utrata danych wymuszają energochłonne odtwarzanie zasobów	Test teoretyczny z wynikiem generowanym automatycznie
	wyjaśnia znaczenie poufności, integralności i dostępności danych;	Test teoretyczny z wynikiem generowanym automatycznie
	określa znaczenie higieny cyfrowej dla bezpiecznego, uporządkowanego i ograniczającego straty danych korzystania z zasobów cyfrowych w pracy zawodowej i biznesowej;	Test teoretyczny z wynikiem generowanym automatycznie
	Wyjaśnia wpływ technologii cyfrowych na środowisko i energetyczny bilans firmy.	Test teoretyczny z wynikiem generowanym automatycznie
	Charakteryzuje rolę cyberbezpieczeństwa w utrzymaniu trwałości infrastruktury cyfrowej.	Test teoretyczny z wynikiem generowanym automatycznie
	Wskazuje mechanizmy ochrony przed malware, które zapobiegają uszkodzeniom sprzętu, wydłużając jego cykl życia	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Umiejętności: Dobiera działania ograniczające ryzyko utraty danych, infekcji złośliwym oprogramowaniem oraz nieuprawnionego dostępu.	dobiera zasady tworzenia i przechowywania haseł do opisanej sytuacji;	Test teoretyczny z wynikiem generowanym automatycznie
	wybiera działania ograniczające ryzyko infekcji;	Test teoretyczny z wynikiem generowanym automatycznie
	dobiera zasady bezpiecznego korzystania z poczty elektronicznej i Internetu.	Test teoretyczny z wynikiem generowanym automatycznie
	Dobiera parametry retencji danych i uprawnień dostępu, które eliminują zbędną duplikację plików i optymalizują serwery	Test teoretyczny z wynikiem generowanym automatycznie
Umiejętności: Ocenia skutki środowiskowe incydentów i dobiera działania naprawcze o niskim wpływie ekologicznym.	identyfikuje elementy wiadomości lub strony wskazujące na phishing albo socjotechnikę;	Test teoretyczny z wynikiem generowanym automatycznie
	określa możliwe skutki incydentu dla ciągłości pracy;	Test teoretyczny z wynikiem generowanym automatycznie
	wskazuje zasoby cyfrowe wymagające zabezpieczenia lub odtworzenia.	Test teoretyczny z wynikiem generowanym automatycznie
	Analizuje na przykładzie wpływ awarii na intensywność pracy sieci i wskazuje kroki ograniczające marnotrawstwo zasobów IT	Test teoretyczny z wynikiem generowanym automatycznie
Umiejętności: Dobiera rozwiązania cyberbezpieczeństwa wspierające ograniczanie strat danych i racjonalne wykorzystanie infrastruktury IT.	dobiera sposób zarządzania dostępami do opisanej sytuacji;	Test teoretyczny z wynikiem generowanym automatycznie
	wybiera zasady tworzenia kopii zapasowych ograniczające ryzyko utraty danych;	Test teoretyczny z wynikiem generowanym automatycznie
	Projektuje zasobooszczędne procedury ochrony zasobów cyfrowych i komunikacji.	Test teoretyczny z wynikiem generowanym automatycznie
	Wybiera postawy prośrodowiskowe w codziennej higienie cyfrowej, promując model energooszczędnego pracownika	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Umiejętności: Dobiera podstawowe zasady reagowania na incydent i bezpiecznej organizacji pracy cyfrowej.	porządkuje działania przed incydentem, w trakcie incydentu i po jego zakończeniu;	Test teoretyczny z wynikiem generowanym automatycznie
	dobiera zasady bezpiecznej pracy zdalnej, korzystania z urządzeń mobilnych i współdzielonych zasobów;	Test teoretyczny z wynikiem generowanym automatycznie
	wybiera rekomendację ograniczającą ryzyko ponownego wystąpienia incydentu	Test teoretyczny z wynikiem generowanym automatycznie
	wskazuje konsekwencje niezgłaszania incydentów;	Test teoretyczny z wynikiem generowanym automatycznie
Kompetencje społeczne: Wykazuje odpowiedzialność za środowisko poprzez stosowanie zasad zrównoważonego korzystania z technologii.	wybiera zachowania chroniące dane i współdzieloną infrastrukturę cyfrową;	Test teoretyczny z wynikiem generowanym automatycznie
	wybiera działania świadczące o odpowiedzialnym korzystaniu z danych, urządzeń i komunikacji cyfrowej, ograniczające ryzyko utraty danych, przestojów i niepotrzebnego odtwarzania zasobów.	Test teoretyczny z wynikiem generowanym automatycznie

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/

Strona internetowa Instytucji Walidującej: https://my-ps.eu/

Informacje

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

Program

Szkolenie prowadzi do nabycia kwalifikacji " Animator Cyberbezpieczeństwa"

Organizator zapewnia salę szkoleniową przystosowaną do realizacji zajęć komputerowych oraz nabywania kompetencji cyfrowych. Sala wyposażona jest w rzutnik multimedialny oraz dostęp do internetu. Uczestnicy pracują przy stolikach w komfortowych warunkach, umożliwiających swobodną pracę indywidualną oraz wsparcie ze strony prowadzącego.

Każdy uczestnik ma zapewnione stanowisko pracy.

W harmonogramie uwzględniono przerwy, które wliczają się do czasu trwania szkolenia.

Walidacja wliczona jest do czasu trwania szkolenia.

ROZDZIELNOŚĆ WALIDACJI: Proces walidacji jest prowadzony z zachowaniem zasady rozdzielności funkcji. Osoba prowadząca szkolenie nie uczestniczy w procesie oceny efektów uczenia się uczestników. Walidację przeprowadza osoba niezaangażowana w realizację usługi szkoleniowej.

PROGRAM USŁUGI

1. Fundamenty cyberbezpieczeństwa i analiza wpływu incydentów na bilans energetyczny (2:30h)

- **Teoria (1:00h):** Systematyzacja wiedzy o współczesnych zagrożeniach sieciowych oraz ich korelacja ze specyfiką operacyjną sektora MŚP i użytkowników indywidualnych.
- **Praktyka (1:30h):** Warsztatowa analiza skutków naruszeń bezpieczeństwa dla ciągłości procesów cyfrowych. Uczestnik ocenia wpływ awarii na nadmiarowe wykorzystanie zasobów sprzętowych oraz bilans energetyczny przedsiębiorstwa, projektując działania minimalizujące koszty środowiskowe wynikające z konieczności energochłonnego odtwarzania danych i powtarzania procesów.

2. Higiena cyfrowa w organizacji jako narzędzie zasobooszczędności IT (3:00h)

- **Teoria (1:00h):** Kluczowe paradygmaty cyberbezpieczeństwa oraz rola higieny cyfrowej w budowaniu zrównoważonej i bezpiecznej kultury organizacyjnej.
- **Praktyka (2:00h):** Implementacja standardów higieny cyfrowej ukierunkowanych na redukcję śladu węglowego technologii. Uczestnik projektuje procedury ograniczające nadmiarowe składowanie informacji, zbędną duplikację plików oraz niekontrolowane przetwarzanie danych, co realnie optymalizuje obciążenie serwerów i zużycie energii przez infrastrukturę IT.

3. Odporność cyfrowa a trwałość infrastruktury i oszczędność zasobów (1:00h)

- **Teoria (0:30h):** Zarządzanie tożsamością, planowanie reakcji na incydenty oraz techniki ochrony przed złośliwym oprogramowaniem w celu zapewnienia ciągłości procesów niskoemisyjnych.
- **Praktyka (0:30h):** Dobór mechanizmów obronnych wydłużających użyteczność sprzętu IT poprzez prewencję uszkodzeń systemowych. Uczestnik planuje działania zapobiegające przestojom, które wymuszają masowe, wysokoenergetyczne odtwarzanie zasobów cyfrowych generujące nadmiarowe obciążenie urządzeń, przepustowości sieci oraz przestrzeni dyskowe

4.Podsumowanie i konsultacje - 0:30 godziny teoretyczne

Usystematyzowanie wiedzy o zagrożeniach sieciowych i zasadach higieny cyfrowej, kładąc szczególny nacisk na analizę ich wpływu na ciągłość procesów biznesowych oraz efektywne wykorzystanie zasobów sprzętowych i energetycznych firmy.

5. Ochrona przed phishingiem i socjotechniką oraz podstawy bezpiecznej pracy zdalnej, szyfrowanie danych i bezpieczeństwo sieci – 2:30 godziny, w tym 1:30 godziny teoretyczne i 1 godzina praktyczna.

Bezpieczna organizacja pracy zdalnej z wykorzystaniem współdzielonych zasobów cyfrowych i dokumentów, ograniczająca potrzebę wielokrotnego przesyłania plików, duplikowania danych i odtwarzania utraconych informacji.

6. Zarządzanie urządzeniami mobilnymi a trwałość technologii i odporność systemowa (1:00h)

- **Teoria (0:30h):** Wprowadzenie do bezpieczeństwa systemów mobilnych, polityki MDM (Mobile Device Management) oraz planowanie scenariuszy reakcji na zagrożenia w środowisku rozproszonym.
- **Praktyka (0:30h):** Symulacja ataków i procedury naprawcze. Uczestnik wdraża mechanizmy zarządzania aktualizacjami i uprawnieniami, które realnie wydłużają cykl życia sprzętu IT, ograniczają awaryjność fizyczną urządzeń i sprzyjają racjonalnemu wykorzystaniu infrastruktury w modelu gospodarki obiegu zamkniętego .

7. Optymalizacja zasobów cyfrowych i fundament zielonej transformacji IT (1:30h)

- **Teoria (1:00h):** Analiza cyberbezpieczeństwa jako elementu efektywności operacyjnej. Badanie zależności między odpornością organizacji a redukcją strat mocy obliczeniowej, czasu pracy i przestrzeni dyskowej.
- **Praktyka (0:30h)**: Projektowanie procedur bezpiecznego zarządzania danymi w chmurze i archiwizacji. Uczestnik optymalizuje parametry retencji i kopii zapasowych w celu ograniczenia nadmiarowego przetwarzania informacji, co bezpośrednio redukuje konsumpcję energii. Warsztat obejmuje dobór zabezpieczeń chroniących procesy przed incydentami wymuszającymi energochłonne odtwarzanie systemów, podkreślając rolę technologii ICT w zielonej transformacji przedsiębiorstw województwa śląskiego.

8.Walidacja - 1 godzina

Walidacja jest przeprowadzana na końcu szkolenia, w ostatnim dniu usługi, i jest wliczona w czas trwania usługi.

Metoda walidacji efektów uczenia się: Test teoretyczny z wynikiem generowanym automatycznie.

Test teoretyczny będzie miał formę pytań sytuacyjnych opartych na przypadkach dotyczących phishingu, utraty danych, awarii urządzenia, organizacji kopii zapasowych, zarządzania dostępami oraz bezpiecznej pracy zdalnej. Uczestnik wybiera rozwiązanie adekwatne do opisanego ryzyka, jego skutków dla ciągłości procesu cyfrowego oraz wykorzystania zasobów IT.

Uczestnicy pracują na swoim sprzęcie.

Warunki organizacyjne:

Szkolenie realizowane jest w formie stacjonarnej w sali szkoleniowej, co umożliwia bezpośrednią interakcję z prowadzącym oraz pracę warsztatową.

Dostawca zapewnia pomieszczenia spełniające bezpieczne i higieniczne warunki realizacji usług, wyposażone w stanowiska z dostępem do zasilania sieciowego dla każdego uczestnika.

Uczestnicy pracują na własnych komputerach przenośnych (laptopy). Organizator zapewnia stabilne bezprzewodowe połączenie z siecią Internet (Wi-Fi) niezbędne do realizacji ćwiczeń praktycznych.

Każdy uczestnik powinien posiadać dostęp do poczty elektronicznej oraz aktualną przeglądarkę internetową w celu logowania się do materiałów i narzędzi wspomagających szkolenie.

Informacje dodatkowe do programu:

Usługa jest powiązana z Regionalną Strategią Innowacji Województwa Śląskiego 2030 poprzez rozwój kompetencji w obszarze inteligentnej specjalizacji **Technologie informacyjne i komunikacyjne** oraz realizację kierunku dotyczącego **inkluzywnej transformacji cyfrowej gospodarki i społeczeństwa regionu**.

Szkolenie rozwija umiejętności rozpoznawania zagrożeń cyfrowych, ochrony danych, urządzeń, komunikacji i dostępu do zasobów cyfrowych, reagowania na incydenty oraz bezpiecznej organizacji pracy zdalnej i mobilnej. Kompetencje te wspierają bezpieczne wykorzystywanie technologii informacyjno-komunikacyjnych przez pracowników i MŚP, ograniczają ryzyko utraty danych, przestojów procesów cyfrowych oraz konieczności odtwarzania danych i ponownego wykonywania pracy.

Powiązanie usługi z inteligentną specjalizacją „Zielona gospodarka” polega na rozwijaniu kompetencji umożliwiających ograniczanie strat zasobów cyfrowych i infrastrukturalnych w przedsiębiorstwie. Uczestnik analizuje skutki incydentów dla danych, urządzeń i ciągłości pracy oraz dobiera działania ograniczające utratę danych, przestoje, zbędne duplikowanie plików i konieczność ich odtwarzania. Kompetencje te wspierają bardziej efektywne wykorzystanie zasobów cyfrowych, sprzętu IT i usług sieciowych w działalności przedsiębiorstw.

Harmonogram

Liczba pozycji harmonogramu: 15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 15 Podstawowe zasady bezpieczeństwa - rozmowa na żywo, ćwiczenia	Zajęcia	BARTOSZ MITERA	04-10-2026	09:00	10:00	01:00
2 z 15 Zagrożenia w sieci i ich wpływ na firmy MŚP	Zajęcia	BARTOSZ MITERA	04-10-2026	10:00	11:30	01:30
3 z 15 -	Przerwa	-	04-10-2026	11:30	12:15	00:45
4 z 15 Podstawowe terminy i koncepcje bezpieczeństwa	Zajęcia	BARTOSZ MITERA	04-10-2026	12:15	13:45	01:30
5 z 15 Higiena cyfrowa w biznesie	Zajęcia	BARTOSZ MITERA	04-10-2026	13:45	15:15	01:30
6 z 15 -	Przerwa	-	04-10-2026	15:15	15:30	00:15
7 z 15 Podsumowanie dnia i konsultacje	Zajęcia	BARTOSZ MITERA	04-10-2026	15:30	16:00	00:30
8 z 15 Hasła, zarządzanie nimi i reagowanie na incydenty	Zajęcia	BARTOSZ MITERA	11-10-2026	09:00	10:00	01:00
9 z 15 Ochrona przed malware, phishing i socjotechnika	Zajęcia	BARTOSZ MITERA	11-10-2026	10:00	11:30	01:30
10 z 15 -	Przerwa	-	11-10-2026	11:30	12:15	00:45

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
11 z 15 Praca zdalna, szyfrowanie i bezpieczeństwo sieci	Zajęcia	BARTOSZ MITERA	11-10-2026	12:15	13:15	01:00
12 z 15 Bezpieczeństwo mobilne i polityki bezpieczeństwa	Zajęcia	BARTOSZ MITERA	11-10-2026	13:15	14:15	01:00
13 z 15 Optymalizacja zasobów i efektywność energetyczna IT	Zajęcia	BARTOSZ MITERA	11-10-2026	14:15	15:45	01:30
14 z 15 -	Przerwa	-	11-10-2026	15:45	16:00	00:15
15 z 15 -	Walidacja	-	11-10-2026	16:00	17:00	01:00

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	15:00
w tym suma godzin zajęć	12:00
w tym suma godzin walidacji	01:00
w tym suma przerw	02:00
Suma godzin dydaktycznych bez przerw	17:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 200,00 PLN

Podmiot uprawniony do zwolnienia z VAT na podstawie art. 113 ust. 1 ustawy o VAT ze względu na wartość sprzedaży

Koszt przypadający na 1 uczestnika netto	5 200,00 PLN
Koszt osobogodziny brutto	346,67 PLN
Koszt osobogodziny netto	346,67 PLN
W tym koszt walidacji brutto	125,00 PLN
W tym koszt walidacji netto	125,00 PLN
W tym koszt certyfikowania brutto	125,00 PLN
W tym koszt certyfikowania netto	125,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	15:00

Prowadzący

Liczba prowadzących: 1

1 z 1

BARTOSZ MITERA

Specjalista ds. Cyberbezpieczeństwa.
Zawodowo związany z bezpieczeństwem IT. Posiada szerokie kompetencje potwierdzone certyfikatami prestiżowych instytucji.
Doświadczenie zawodowe oraz umiejętności trenera zostały nabyte w okresie 5 lat poprzedzających realizację usługi. Jako trener łączy wiedzę techniczną z zakresu sieci komputerowych i AI z praktycznymi wyzwaniami sektora MŚP, w tym transformacją cyfrową oraz efektywnością energetyczną. Szkolenia koncentrują się na budowaniu fundamentów bezpieczeństwa i nowoczesnym e-commerce.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały szkoleniowe: Prezentacja w wersji elektronicznej przekazywane w pierwszym dniu szkolenia.

- Wymagana frekwencja na zajęciach wynosi **minimum 80%** godzin dydaktycznych.
- Uczestnik otrzymuje komplet materiałów szkoleniowych w formie cyfrowej, w tym: autorskie skrypty.
- Usługa kończy się uzyskaniem certyfikatu potwierdzającego nabycie kwalifikacji zawodowych: **Animator Cyberbezpieczeństwa**."

Sala szkoleniowa i warunki organizacyjne

Zgodnie z opisem programu, organizator zapewnia profesjonalne zaplecze techniczne dostosowane do specyfiki szkolenia z cyberbezpieczeństwa:

- Wyposażenie: Sala jest przystosowana do zajęć komputerowych, wyposażona w rzutnik multimedialny oraz stabilne, bezprzewodowe połączenie z siecią Internet (Wi-Fi).
- Stanowiska pracy: Każdy uczestnik ma zapewnione indywidualne, samodzielne stanowisko pracy przy stoliku w komfortowych warunkach, co umożliwia zarówno swobodną pracę własną, jak i wsparcie trenera.
- Sprzęt: Uczestnicy pracują na własnych komputerach przenośnych

Adres

ul. Obrzeżna Północna 22

41-400 Mysłowice

woj. śląskie

Zajęcia odbywają się w Mysłowicach przy ul. Obrzeżna północna 22

Sala szkoleniowa i warunki organizacyjne
Zgodnie z opisem programu, organizator zapewnia profesjonalne zaplecze techniczne dostosowane do specyfiki szkolenia z cyberbezpieczeństwa:
Wyposażenie: Sala jest przystosowana do zajęć komputerowych, wyposażona w rzutnik multimedialny oraz stabilne, bezprzewodowe połączenie z siecią Internet (Wi-Fi).
Stanowiska pracy: Każdy uczestnik ma zapewnione indywidualne, samodzielne stanowisko pracy przy stoliku w komfortowych warunkach, co umożliwia zarówno swobodną pracę własną, jak i wsparcie trenera.
Sprzęt: Uczestnicy pracują na własnych komputerach przenośnych (laptopy), natomiast dostawca zapewnia dostęp do zasilania sieciowego dla każdego stanowisk.

Udogodnienia w miejscu realizacji usługi

- Wi-fi

Kontakt

Teresa Węglarz

E-mail futureskills.biuro@gmail.com
Telefon (+48) 510 488 540