Możliwość dofinansowania

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

Numer usługi 2026/06/01/217047/3602310

5 250,00 PLN brutto
5 250,00 PLN netto
350,00 PLN brutto/h
350,00 PLN netto/h
261,33 PLN cena rynkowa

Future Skills Teresa Węglarz

Brak ocen dla tego dostawcy

Sosnowiec
Usługa szkoleniowa
stacjonarna
Zajęcia grupowe
15:00 h
25.07.2026 do 28.07.2026

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	23-07-2026
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

Usługa przygotowuje do rozpoznawania zagrożeń cyfrowych, stosowania zasad higieny cyfrowej, ochrony danych, urządzeń i komunikacji, reagowania na podstawowe incydenty bezpieczeństwa w środowisku firmy i indywidualnym. Uczestnik analizuje wpływ incydentów na ciągłość procesów cyfrowych, wykorzystanie infrastruktury IT i konieczność odtwarzania danych i pracy. Dobiera działania cyberbezpieczeństwa i zasobooszczędne w firmie, w kontekście transformacji cyfrowej i zielonej gospodarki w woj. śląskim.

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.	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
	wskazuje znaczenie aktualizacji, kopii zapasowych i zarządzania dostępem dla ograniczania awarii infrastruktury IT.	Test teoretyczny z wynikiem generowanym automatycznie
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

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Umiejętności: Analizuje sytuację incydentu cyberbezpieczeństwa pod kątem jego skutków dla danych, urządzeń i procesów cyfrowych.	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
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
	dobiera działania ograniczające zbędne duplikowanie plików, przestoje i konieczność odtwarzania zasobów cyfrowych.	Test teoretyczny z wynikiem generowanym automatycznie
	porządkuje działania przed incydentem, w trakcie incydentu i po jego zakończeniu;	Test teoretyczny z wynikiem generowanym automatycznie
Umiejętności: Dobiera podstawowe zasady reagowania na incydent i bezpiecznej organizacji pracy cyfrowej.	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: Ocenia znaczenie odpowiedzialnego postępowania w zakresie ochrony danych, urządzeń i komunikacji cyfrowej dla ograniczania ryzyka incydentów oraz strat zasobów cyfrowych.	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. Zrozumienie podstawowych zasad bezpieczeństwa oraz zagrożenia w sieci i ich wpływ na firmy MŚP i osoby indywidualne – 2:30 godziny, w tym 1 godzina teoretyczna i 1:30 godziny praktyczne.

Analiza skutków incydentów cyberbezpieczeństwa dla ciągłości procesów cyfrowych, konieczności odtwarzania danych, ponownego wykonywania pracy oraz wykorzystania zasobów sprzętowych i energetycznych przedsiębiorstwa.

2. Podstawowe terminy i koncepcje oraz znaczenie higieny cyfrowej w kontekście biznesowym – 3 godziny, w tym 1 godzina teoretyczna i 2 godziny praktyczne.

Zasady higieny cyfrowej ograniczające nadmiarowe przechowywanie, duplikowanie i niekontrolowane przetwarzanie danych w środowisku pracy.

3. Hasła i zarządzanie nimi, przygotowanie planu reagowania na incydenty oraz zaawansowana ochrona przed złośliwym oprogramowaniem i bezpieczne korzystanie z Internetu – 1 godzina, w tym 0:30 godziny teoretyczne i 0:30 godziny praktyczne.

Dobór działań ograniczających ryzyko przestojów, utraty danych i konieczności odtwarzania zasobów cyfrowych, które generują dodatkowe wykorzystanie urządzeń, sieci oraz przestrzeni dyskowej.

4. 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.

5. Wprowadzenie do bezpieczeństwa urządzeń mobilnych i polityki bezpieczeństwa oraz symulacje ataków cybernetycznych i reakcje – 1 godzina, w tym 0:30 godziny teoretyczne i 0:30 godziny praktyczne.

Analiza wpływu właściwego zarządzania urządzeniami, aktualizacjami i dostępami na wydłużanie użyteczności sprzętu IT, ograniczanie awarii oraz racjonalne wykorzystanie infrastruktury cyfrowej.

6. Cyberbezpieczeństwo jako element efektywnego wykorzystania zasobów cyfrowych i infrastruktury IT – 1:30 godziny, w tym 1 godzina teoretyczna i 0:30 godziny praktyczne.

- zależność między cyberodpornością organizacji a ograniczaniem strat danych, czasu pracy, mocy obliczeniowej, przestrzeni dyskowej i urządzeń;
  - zasady bezpiecznego zarządzania danymi w chmurze, kopiami zapasowymi i dostępami z uwzględnieniem ograniczania zbędnego przechowywania danych;
  - analiza sytuacji MŚP: dobór zabezpieczeń chroniących proces cyfrowy przed incydentem powodującym przestój i konieczność odtwarzania danych;
  - znaczenie technologii informacyjno-komunikacyjnych dla cyfrowej i zielonej transformacji przedsiębiorstw w województwie śląskim.

7.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	25-07-2026	09:00	10:00	01:00
2 z 15 Zagrożenia w sieci i ich wpływ na firmy MŚP	Zajęcia	BARTOSZ MITERA	25-07-2026	10:00	11:30	01:30
3 z 15 -	Przerwa	-	25-07-2026	11:30	12:15	00:45
4 z 15 Podstawowe terminy i koncepcje bezpieczeństwa	Zajęcia	BARTOSZ MITERA	25-07-2026	12:15	13:45	01:30
5 z 15 Higiena cyfrowa w biznesie	Zajęcia	BARTOSZ MITERA	25-07-2026	13:45	15:15	01:30
6 z 15 -	Przerwa	-	25-07-2026	15:15	15:30	00:15
7 z 15 Podsumowanie dnia i konsultacje	Zajęcia	BARTOSZ MITERA	25-07-2026	15:30	16:00	00:30
8 z 15 Hasła, zarządzanie nimi i reagowanie na incydenty	Zajęcia	BARTOSZ MITERA	26-07-2026	09:00	10:00	01:00
9 z 15 Ochrona przed malware, phishing i socjotechnika	Zajęcia	BARTOSZ MITERA	26-07-2026	10:00	11:30	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
10 z 15 -	Przerwa	-	26-07-2026	11:30	12:15	00:45
11 z 15 Praca zdalna, szyfrowanie i bezpieczeństwo sieci	Zajęcia	BARTOSZ MITERA	26-07-2026	12:15	13:15	01:00
12 z 15 Bezpieczeństwo mobilne i polityki bezpieczeństwa	Zajęcia	BARTOSZ MITERA	26-07-2026	13:15	14:15	01:00
13 z 15 Optymalizacja zasobów i efektywność energetyczna IT	Zajęcia	BARTOSZ MITERA	26-07-2026	14:15	15:45	01:30
14 z 15 -	Przerwa	-	26-07-2026	15:45	16:00	00:15
15 z 15 -	Walidacja	-	26-07-2026	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	5 250,00 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	5 250,00 PLN
Koszt osobogodziny brutto	350,00 PLN
Koszt osobogodziny netto	350,00 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 od 2025 roku. 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.

Adres

Sosnowiec
Sosnowiec
woj. śląskie

Kontakt

Teresa Węglarz

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