



Cyberbezpieczeństwo i ochrona danych w przedsiębiorstwie

Numer usługi 2025/12/04/15085/3191362

2 100,00 PLN brutto

2 100,00 PLN netto

175,00 PLN brutto/h

175,00 PLN netto/h

CENTRUM
NAUCZANIA "LET'S
GO" Nazwa
skrótowa CN " LET'S
GO" KACPRZAK
MIROSŁAWA

★★★★★ 4,7 / 5

57 ocen

📍 zdalna w czasie rzeczywistym

👤 Usługa szkoleniowa

🕒 12 h

📅 10.03.2026 do 13.03.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikatory projektów	Regionalny Fundusz Szkoleniowy II
Grupa docelowa usługi	Usługa skierowana jest do właścicieli mikroprzedsiębiorstw i przedstawicieli MŚP oraz innych osób dorosłych, które w ramach swoich wykonywanych czynności zawodowych potrzebują poznać bezpieczne techniki ochrony pracy w sieci
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	6
Data zakończenia rekrutacji	09-03-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	12
Podstawa uzyskania wpisu do BUR	Certyfikat ICVC - SURE (Standard Usług Rozwojowych w Edukacji): Norma zarządzania jakością w zakresie świadczenia usług rozwojowych

Cel

Cel edukacyjny

Szkolenie " Cyberbezpieczeństwo i ochrona danych w przedsiębiorstwie" przygotowuje do samodzielnego działania w zakresie ochrony danych i bezpieczeństwa cyfrowego w mikroprzedsiębiorstwach oraz sektorze MŚP oraz rozpoznawania zagrożeń cybernetycznych, skutecznej ochrony danych i urządzeń w codziennej pracy.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
charakteryzuje podstawowe zagrożenia cyfrowe w mikro i MŚP	definiuje aktualne zagrożenia w Polsce i na świecie	Obserwacja w warunkach rzeczywistych
	rozpoznaje i klasyfikuje przykłady ataków phishingowych, ransomware i innych zagrożeń	Obserwacja w warunkach rzeczywistych
planuje zasady bezpiecznej pracy zdanyimi i urządzeniami	definiuje podstawy prawne i standardy bezpieczeństwa w firmie	Obserwacja w warunkach rzeczywistych
	opracowuje zasady zarządzania nośnikami danych	Obserwacja w warunkach rzeczywistych
Rozróżnia bezpieczne i niebezpieczne praktyki w zakresie zarządzania hasłami i kontami.	opracowuje uwierzytelniające hasła oraz wskazuje elementy wymagające poprawy w zabezpieczeniu haseł	Obserwacja w warunkach rzeczywistych
Opracowuje metody pracy zgodne z podstawowymi zasadami bezpieczeństwa systemów i urządzeń	stosuje ustawienia zabezpieczeń i aktualizacji	Obserwacja w warunkach rzeczywistych
Stosuje metody bezpiecznej komunikacji online oraz ochrony tożsamości cyfrowej	stosuje odpowiednie działania w przypadku podejrzenia phishingu, fałszywych źródeł lub naruszenia prywatności.	Obserwacja w warunkach rzeczywistych

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

TAK

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Szkolenie jest adresowane dla osób potrzebujących poznać bezpieczne techniki ochrony pracy w sieci. Realizowane będzie w jednej grupie szkoleniowej w formie zdalnej. Każdy uczestnik będzie pracował przy swoim stanowisku komputerowym. Łączna liczba godzin szkolenia zawiera 12 h dydaktycznych (1 h dydaktyczna = 45 minut) - 8 h zajęć teoretycznych i 4 h zajęć praktycznych . Po każdych 2 h zajęć przewidywana jest przerwa -15 minut , nie wliczana do czasu zajęć. Po zakończonym szkoleniu odbędzie się test składający się z pytań zamkniętych opracowanych przez zewnętrznego egzaminatora. Czas trwania testu -45 minut. program szkolenia obejmuje następujące zagadnienia :

Podstawowe pojęcia i cele cyberbezpieczeństwa

Identyfikacja współczesnych zagrożeń w sieci

Konsekwencje naruszeń bezpieczeństwa

Najczęstsze techniki ataków cyberprzestępców

2.Zasady bezpiecznej pracy z danymi i urządzeniami

Ochrona haseł i kont

Zasady tworzenia bezpiecznych haseł

3.Zarządzanie hasłami i kontami

Strategie zarządzania wieloma kontami

Wykorzystanie menedżerów haseł

4.Podstawowe zasady bezpieczeństwa

Bezpieczeństwo urządzeń

System aktualizacji oprogramowania

Konfiguracja zabezpieczeń systemowych

Zarządzanie uprawnieniami dostępu

Ochrona przed złośliwym oprogramowaniem

4. Metody bezpiecznej komunikacji online oraz ochrony tożsamości

Bezpieczna komunikacja online

Weryfikacja wiarygodności źródeł

Rozpoznawanie prób phishingu

Bezpieczne korzystanie z poczty elektronicznej

Ochrona prywatności w mediach społecznościowych

WALIDACJA EFEKTÓW UCZENIA SIĘ

Harmonogram

Liczba przedmiotów/zajęć: 0

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 100,00 PLN
Koszt przypadający na 1 uczestnika netto	2 100,00 PLN
Koszt osobogodziny brutto	175,00 PLN
Koszt osobogodziny netto	175,00 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Mariusz Szczubiał

Doradca i szkoleniowiec w obszarze cyberbezpieczeństwa i ochrony danych . Absolwent Akademii im. Leona Koźmińskiego w Warszawie - Podyplomowe Studia Ochrona danych osobowych ukończone w 2022r.W ciągu ostatnich 3 lat przeprowadził kilkadziesiąt szkoleń z cyberbezpieczeństwa dla pracowników samorządowych oraz przedsiębiorców

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymają dostęp do materiałów szkoleniowych w formie elektronicznej- skrypt z zakresu programu szkolenia, ćwiczenia

Warunki uczestnictwa

Uczestnicy nie muszą wykazywać się minimalnym doświadczeniem aby uczestniczyć w usłudze rozwojowej

Dostawca usługi zapewnia realizację usługi rozwojowej uwzględniając potrzeby osób z niepełnosprawnościami (w tym również dla osób ze szczególnymi potrzebami) zgodnie ze Standardami dostępności dla polityki spójności 2021-2027

Informacje dodatkowe

Warunkiem uzyskania zaświadczenia jest uczestnictwo w co najmniej 80% zajęć usługi rozwojowej

Zapisując się na usługę wyrażasz zgodę na rejestrowanie/nagrywanie swojego wizerunku na potrzeby monitoringu, kontroli oraz w celu utrwalenia efektów uczenia się.

Ocena efektów uczenia się prowadzona jest za pośrednictwem obserwacji w warunkach rzeczywistych przez oddzielnego walidatora - zchowana jest rozdzielnosc szkoleń - walidacja

Szkolenie realizowane jest również dla uczestników projektów :

Fundusz Szkoleniowy II

Kierunek- Rozwój - podpisana umowa z WUP w Toruń

Zachodniopomorski bon szkoleniowy - podpisana umowa z WUP Szczecin

Warunki techniczne

Szkolenie będzie odbywać się w formie on-line za pomocą platformy Google Meet

1. W celu prawidłowego i pełnego korzystania z platformy Uczestnik powinien dysponować:

urządzeniem mającym dostęp do sieci Internet (komputer, smartfon, tablet),

zdolnym do odbioru i przekazu dźwięku (głośniki, słuchawki, mikrofon), przeglądarką Windows: Edge 12+, Firefox 27+, Chrome 30+,Mac:Safari 7+, Firefox 27+, Chrome 30+,

kamerką internetową.

2. Minimalna wymagana szybkość połączenia internetowego w celu korzystania z webinarów wynosi 2 Mb/s (zalecane połączenie szerokopasmowe).

3. Dołączenie następuje poprzez kliknięcie w indywidualny link wysłany mailem do uczestnika przed szkoleniem oraz wpisanie imienia i nazwiska w oknie logowania.

4.Trzy dni przed rozpoczęciem szkolenia udostępniony zostanie link wysłany również mailem do wszystkich uczestników szkolenia

5. Ważność linku - od rozpoczęcia szkolenia do jego zakończenia zgodnie z harmonogramem w karcie.

Kontakt



Mirosława Kacprzak

E-mail cn.centrum@gmail.com

Telefon (+48) 513 104 504