Możliwość dofinansowania

Cyberbezpieczeństwo dla firm - bezpieczne zarządzanie dokumentami, hasłami i zwiększanie świadomości socjotechniki

Numer usługi 2026/03/06/40363/3387219

174,66 PLN brutto
142,00 PLN netto
24,95 PLN brutto/h
20,29 PLN netto/h
261,33 PLN cena rynkowa

Instytut Doskonałości Strategicznej Sp. z o.o.

5,0 / 5

1 261 ocen

Chełmno
Usługa szkoleniowa
stacjonarna
07:00 h
24.06.2026 do 24.06.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikatory projektów	Regionalny Fundusz Szkoleniowy II
Grupa docelowa usługi	Przedsiębiorcy i pracownicy świadczący usługi w rolnictwa, którzy chcą pozyskać rozwiązania i propozycje w zakresie cyberbezpieczeństwa.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	21
Data zakończenia rekrutacji	23-06-2026
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	7
Podstawa uzyskania wpisu do BUR	Znak Jakości Małopolskich Standardów Usług Edukacyjno-Szkoleniowych (MSUES) - wersja 2.0

Cel

Cel edukacyjny

Usługa przygotowuje uczestnika do samodzielnego działania w zakresie zapewnienia bezpieczeństwa danych osobowych oraz informacji poufnych.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik po zakończonej usłudze posługuje się wiedzą dotyczącą: - cyberbezpieczeństwa, - odpowiedzialności za ochronę danych osobowych i poufnych oraz zasad związanych z RODO i ustawą o krajowym systemie cyberbezpieczeństwa, - różnorodnych zagrożeń, najlepszych praktyk bezpieczeństwa danych oraz przepisów dotyczących ochrony danych osobowych.	Uczestnik po zakończonej usłudze: - definiuje i opisuje cyberbezpieczeństwo, - omawia rodzaje cyberzagrożeń i ocenia ich skutki, - omawia zasady odpowiedzialności za ochronę danych osobowych i poufnych oraz związanych z RODO i ustawą o krajowym systemie cyberbezpieczeństwa, - omawia różnorodne zagrożenia, - odczytuje zasady najlepszych praktyk bezpieczeństwa danych oraz przepisów dotyczących ochrony danych osobowych.	Test teoretyczny
Uczestnik po zakończonej usłudze: - charakteryzuje ryzyko związane z cyberatakami, identyfikuje słabe punkty w systemach i procedurach bezpieczeństwa, - stosuje techniki zapobiegania atakom i reagowania na incydenty, - przygotowuje plany zarządzania ryzykiem i strategie reagowania na incydenty.	Uczestnik po zakończonej usłudze: - omawia ryzyko związane z cyberatakami, identyfikuje słabe punkty w systemach i procedurach bezpieczeństwa; - omawia różorodne techniki zapobiegania atakom i reagowania na incydenty, - wykonuje zarys planu zarządzania ryzykiem i strategie reagowania na incydenty.	Test teoretyczny
Uczestnik po zakończonej usłudze: - organizuje współpracę i komunikację w zakresie bezpieczeństwa danych oraz promowanie kultury bezpieczeństwa.	Uczestnik po zakończonej usłudze: - omawia zasady współpracy i komunikacji w zakresie berbezpieczeństwa danych oraz promowania kultury bezpieczeństwa.	Test teoretyczny

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

W trakcie usługi szkoleniowej zostaną podjęte następujące zagadnienia umożliwiające zdobycie i usystematyzowanie przewidzianych w usłudze zasobów wiedzy, umiejętności i społecznych kompetencji w zakresie cyberbezpieczeństwa:

- Zapoznanie uczestników z celami i metodami prowadzenia szkolenia, a także jego zakładanymi efektami oraz wprowadzenie do szkolenia;
- Definicja i zakres cyberbezpieczeństwa;
- Rodzaje cyberzagrożeń i ich skutki;
- Dlaczego cyberbezpieczeństwo jest ważne?;
- Rodzaje przetwarzanych danych i usług;
- Odpowiedzialność za ochronę danych osobowych i poufnych;
- Zasady RODO i ustawy o krajowym systemie cyberbezpieczeństwa;
- Przykłady ataków i sposoby ochrony;
- Zasady tworzenia i zarządzania hasłami;
- Zasady aktualizacji i zabezpieczania systemów i aplikacji;
- Zasady bezpiecznej komunikacji i współpracy online;
- Zasady postępowania w przypadku podejrzenia lub wykrycia incydentu;
- Jak rozpoznawać ataki phishingowe?;
- Metody socjotechniczne używane przez hakerów;
- Test z rozpoznawania ataków phishingowych;
- Walidujący test teoretyczny.

Szkolenie adresowane jest do przedsiębiorców i pracowników świadczący usługi świadczący usługi w zakresie rolnictwa.

Usługa jest realizowana w godzinach zegarowych.

Zaplanowane przerwy wliczają się w czas trwania usługi. Przerwy będą uzgadniane indywidualnie z uczestnikami szkolenia.

Harmonogram

Liczba pozycji harmonogramu: 13

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 13 Zapoznanie uczestników z celami i metodami prowadzenia szkolenia, a także jego zakładanymi efektami oraz wprowadzenie do szkolenia	Adrian Iwanek	24-06-2026	08:00	08:15	00:15

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
2 z 13 Czym jest cyberbezpieczeństwo: • Definicja i zakres, • rodzaje cyber- zagrożeń i ich skutki, • przykłady ataków na systemy informatyczne i dane	Adrian Iwanek	24-06-2026	08:15	08:45	00:30
3 z 13 Rodzaje przetwarzanych danych i usług oraz odpowiedzialność za ochronę danych osobowych i poufnych	Adrian Iwanek	24-06-2026	08:45	09:30	00:45
4 z 13 Rodzaje przetwarzanych danych i usług oraz odpowiedzialność za ochronę danych osobowych i poufnych	Adrian Iwanek	24-06-2026	09:30	10:00	00:30
5 z 13 Przerwa	Adrian Iwanek	24-06-2026	10:00	10:15	00:15
6 z 13 Zasady RODO i ustawy o krajowym systemie cyberbezpieczeństwa oraz przykłady ataków	Adrian Iwanek	24-06-2026	10:15	10:45	00:30
7 z 13 Zasady tworzenia i zarządzania hasłami oraz zasady aktualizacji i zabezpieczania systemów i aplikacji	Adrian Iwanek	24-06-2026	10:45	11:15	00:30

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
8 z 13 Zasady bezpiecznej komunikacji i współpracy online oraz zasady postępowania w przypadku podejrzenia lub wykrycia incydentu	Adrian Iwanek	24-06-2026	11:15	11:45	00:30
9 z 13 Rozpoznawanie ataków phishingowych	Adrian Iwanek	24-06-2026	11:45	12:45	01:00
10 z 13 Przerwa	Adrian Iwanek	24-06-2026	12:45	13:00	00:15
11 z 13 Metody socjotechniczne używane przez hakerów	Adrian Iwanek	24-06-2026	13:00	13:30	00:30
12 z 13 Test z rozpoznawania ataków phishingowych	Adrian Iwanek	24-06-2026	13:30	14:30	01:00
13 z 13 Walidujący test teoretyczny	-	24-06-2026	14:30	15:00	00:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	174,66 PLN
Koszt przypadający na 1 uczestnika netto	142,00 PLN
Koszt osobogodziny brutto	24,95 PLN
Koszt osobogodziny netto	20,29 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Adrian Iwanek

Posiada wiedzę i doświadczenie zgodne z zakresem tematycznym usługi. Trener posiada rozległą wiedzę zarówno w dziedzinie cyberbezpieczeństwa, jak i w praktycznym wykorzystaniu technologii zabezpieczeń. Jako specjalista z wieloletnim doświadczeniem w dziedzinie programowania i cyberbezpieczeństwa, ma głęboką znajomość wszystkich aspektów bezpieczeństwa informatycznego oraz doskonałą umiejętność praktycznego stosowania narzędzi cyberbezpieczeństwa.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy na bieżąco będą wyposażani w wiedzę (mającą formę ustna i pisemną) oraz materiały niezbędne do realizowania w trakcie szkolenia kolejnych prac warsztatowych, w tym m.in. w ukierunkowane pytania, arkusze analityczne.

Warunki uczestnictwa

Warunkiem uczestnictwa w usłudze szkoleniowej jest poprawne zarejestrowanie przez przedsiębiorcę usługi poprzez system Bazy Usług Rozwojowych.

Informacje dodatkowe

Forma wsparcia po zakończonej usłudze: możliwość dodatkowych konsultacji w formie mailowej i telefonicznej.

Usługodawca dopuszcza przesunięcie przerw w czasie na zgodne życzenie wszystkich uczestników.

Ankieta oceniająca na koniec usługi (element obligatoryjny).

Adres

ul. Przemysłowa 6
86-200 Chełmno
woj. kujawsko-pomorskie

ul. Przemysłowa 6, 86-200 Chełmno

Udogodnienia w miejscu realizacji usługi

- Wi-fi

Kontakt

Waldemar Glabiszewski

E-mail ids@ids-umk.pl

Telefon (+48) 604 235 663