Możliwość dofinansowania

Podstawy cyberbezpieczeństwa w organizacji

Numer usługi 2026/05/04/41749/3533109

3 180,00 PLN brutto
3 180,00 PLN netto
198,75 PLN brutto/h
198,75 PLN netto/h
261,33 PLN cena rynkowa

Pośrednictwo Biznesowe Maciej Pyszka

4,9 / 5

258 ocen

Usługa szkoleniowa
zdalna w czasie rzeczywistym
16:00 h
21.09.2026 do 22.09.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Grupą docelową szkolenia „Podstawy cyberbezpieczeństwa w organizacji” są pracownicy firm i instytucji, którzy na co dzień korzystają z komputerów, systemów informatycznych oraz Internetu i chcą zwiększyć swoje kompetencje w zakresie bezpiecznego przetwarzania informacji. Szkolenie skierowane jest do kadry administracyjnej i biurowej, specjalistów różnych działów, menedżerów oraz osób odpowiedzialnych za obieg dokumentów i danych w organizacji. Adresatami są także przedsiębiorcy oraz właściciele małych i średnich firm, którzy chcą zadbać o bezpieczeństwo informacji w swojej działalności. Grupę docelową stanowią również osoby rozpoczynające pracę zawodową oraz wszyscy pracownicy, którzy chcą zdobyć podstawową wiedzę z zakresu cyberbezpieczeństwa, w tym rozpoznawania zagrożeń, ochrony danych oraz bezpiecznego korzystania z narzędzi cyfrowych.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	20-09-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	16
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

Celem szkolenia „Podstawy cyberbezpieczeństwa w organizacji” jest podniesienie wiedzy i kompetencji uczestników w zakresie rozpoznawania zagrożeń cybernetycznych oraz stosowania podstawowych zasad ochrony danych i systemów informatycznych w środowisku pracy, a także kształtowanie bezpiecznych nawyków w korzystaniu z narzędzi cyfrowych.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik definiuje podstawowe pojęcia z zakresu cyberbezpieczeństwa oraz ochrony informacji.	poprawnie wyjaśnia kluczowe pojęcia (np. cyberbezpieczeństwo, dane, incydent bezpieczeństwa)	Test teoretyczny
	rozróżnia podstawowe obszary bezpieczeństwa informacji	Wywiad swobodny
Uczestnik rozpoznaje najczęstsze zagrożenia cybernetyczne, takie jak phishing, malware czy wycieki danych.	identyfikuje przykłady ataków i zagrożeń	Wywiad swobodny
	wskazuje charakterystyczne cechy prób cyberataków	Wywiad swobodny
Uczestnik stosuje podstawowe zasady bezpiecznego korzystania z poczty elektronicznej, Internetu i systemów firmowych.	stosuje zasady bezpiecznego otwierania załączników i linków	Wywiad swobodny
	korzysta z Internetu i systemów zgodnie z zasadami bezpieczeństwa	Wywiad swobodny
Uczestnik identyfikuje ryzyka związane z niebezpiecznym przetwarzaniem danych w organizacji.	wskazuje sytuacje zagrażające bezpieczeństwu danych	Wywiad swobodny
	ocenia poziom ryzyka w przykładowych scenariuszach	Obserwacja w warunkach symulowanych
Uczestnik stosuje dobre praktyki w zakresie ochrony haseł i dostępu do systemów informatycznych.	tworzy silne i bezpieczne hasła	Wywiad swobodny
	stosuje zasady zarządzania dostępem do kont i systemów	Wywiad swobodny
Uczestnik reaguje właściwie na potencjalne incydenty bezpieczeństwa w środowisku cyfrowym.	opisuje prawidłowe działania w przypadku incydentu	Wywiad swobodny
	wskazuje właściwe osoby lub procedury zgłaszania zagrożeń	Wywiad swobodny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Dzień 1 (09:00–17:00)

09:00–11:00 (2h)

Wprowadzenie do cyberbezpieczeństwa i ochrony informacji

- podstawowe pojęcia i definicje
- znaczenie cyberbezpieczeństwa w organizacji
- rodzaje danych i ich ochrona

11:00–13:00 (2h)

Najczęstsze zagrożenia cybernetyczne

- phishing, malware, ransomware
- socjotechnika i manipulacja
- przykłady incydentów

13:00–13:15 – przerwa

13:15–15:15 (2h)

Bezpieczne korzystanie z systemów i Internetu

- zasady pracy w sieci
- bezpieczna poczta elektroniczna
- ochrona urządzeń i systemów firmowych

15:15–17:15 (2h)

Zajęcia praktyczne: identyfikacja zagrożeń

- analiza przykładów phishingu
- rozpoznawanie podejrzanych wiadomości
- ćwiczenia decyzyjne (bezpieczne/niebezpieczne działania)

Dzień 2 (09:00–17:00)

09:00–11:00 (2h)

Ochrona danych i zarządzanie dostępem

- zasady ochrony danych w organizacji
- bezpieczeństwo haseł
- kontrola dostępu do systemów

11:00–13:00 (2h)

Reagowanie na incydenty bezpieczeństwa

- typy incydentów cyberbezpieczeństwa
- procedury reagowania
- zgłaszanie zagrożeń

13:00–13:15 – przerwa

13:15–15:15 (2h)

Budowanie bezpiecznych nawyków w pracy

- dobre praktyki użytkownika
- minimalizacja ryzyka błędów
- odpowiedzialność pracownika

15:15–16:15 (1h)

Zajęcia praktyczne: scenariusze incydentów

- symulacje ataków i reakcji
- analiza przypadków
- podejmowanie decyzji bezpieczeństwa

16:15–17:15 (1h)

Walidacja efektów uczenia się

Harmonogram

Liczba pozycji harmonogramu: 11

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 11 Wprowadzenie do cyberbezpieczeństwa i ochrony informacji	Klaudia Skelnik	21-09-2026	09:00	11:00	02:00
2 z 11 Najczęstsze zagrożenia cybernetyczne	Klaudia Skelnik	21-09-2026	11:00	13:00	02:00

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
3 z 11 przerwa	Klaudia Skelnik	21-09-2026	13:00	13:15	00:15
4 z 11 Bezpieczne korzystanie z systemów i Internetu	Klaudia Skelnik	21-09-2026	13:15	15:15	02:00
5 z 11 Zajęcia praktyczne: identyfikacja zagrożeń	Klaudia Skelnik	21-09-2026	15:15	17:15	02:00
6 z 11 Ochrona danych i zarządzanie dostępem	Klaudia Skelnik	22-09-2026	09:00	11:00	02:00
7 z 11 Reagowanie na incydenty bezpieczeństwa	Klaudia Skelnik	22-09-2026	11:00	13:00	02:00
8 z 11 przerwa	Klaudia Skelnik	22-09-2026	13:00	13:15	00:15
9 z 11 Budowanie bezpiecznych nawyków w pracy	Klaudia Skelnik	22-09-2026	13:15	15:15	02:00
10 z 11 Zajęcia praktyczne: scenariusze incydentów	Klaudia Skelnik	22-09-2026	15:15	16:15	01:00
11 z 11 Walidacja efektów uczenia się	-	22-09-2026	16:15	17:15	01:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 180,00 PLN

Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT

Koszt przypadający na 1 uczestnika netto	3 180,00 PLN
Koszt osobogodziny brutto	198,75 PLN
Koszt osobogodziny netto	198,75 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Klaudia Skelnik

Prodziekan Wydziału Prawa i Administracji Wyższej Szkoły Bankowej w Gdańsku, doktor nauk społecznych w dyscyplinie nauk o bezpieczeństwie. Absolwentka studiów MBA z zakresu zarządzania bezpieczeństwem, politologii oraz licznych studiów podyplomowych, m.in. z prawa UE, bezpieczeństwa informacji, BHP i edukacji dla bezpieczeństwa. Certyfikowany audytor i pełnomocnik systemów zarządzania bezpieczeństwem informacji (ISO 27001), jakości (ISO 9001) oraz BHP (ISO 45001), posiada bogate doświadczenie we wdrożeniach i audytach w administracji publicznej i sektorze prywatnym. Wiceprezes Pomorskiego Biura Inspektorów Ochrony Danych oraz członek European Association for Security.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały dodatkowe zapewnia realizator:

-case study

-prezentacja

-interaktywne ćwiczenia

Uczestnik otrzyma materiały w dniu szkolenia.

Warunki uczestnictwa

Zapis na usługę z wykorzystaniem odpowiedniego ID wsparcia.

Warunkiem uzyskania zaświadczenia i certyfikatu jest uczestnictwo w 100% szkolenia. Warunkiem niezbędnym do spełnienia przez uczestników, aby realizacja usługi pozwoliła na osiągnięcie głównego celu jest aktywność oraz obecność na szkoleniu.

Informacje dodatkowe

Usługa rozwojowa nie jest świadczona przez podmiot pełniący funkcję Operatora lub Partnera Operatora w danym projekcie PSFlubwktórymkolwiek Regionalnym Programie lub FERS albo przez podmiot powiązany z Operatorem lub Partnerem kapitałowo lub

osobowo. Usługa rozwojowa nie jest świadczona przez podmiot będący jednocześnie podmiotem korzystającym z usług rozwojowych

Usługa rozwojowa nie obejmuje wzajemnego świadczenia usług w projekcie o zbliżonej tematyce przez Dostawców usług, którzy delegują

trwałych przekazywanych Przedsiębiorcom lub Pracownikom przedsiębiorcy, kosztów dojazdu.

Warunki techniczne

Rodzaj komunikatora, za pośrednictwem którego prowadzona będzie usługa rozwojowa: Usługa szkoleniowa realizowana będzie zdalnie w

Minimalne wymagania sprzętowe, jakie musi spełniać komputer Uczestnika lub inne urządzenie do zdalnej komunikacji: Komputer(PClubli

- szerokopasmowe przewodowe lub bezprzewodowe (3G lub4G /LTE)- Głośniki i mikrofon - wbudowany lub wtyk

USB lubbezprzewodowy Bluetooth - Kamera internetowa lub kamera internetowaHD -wbudowana lub wtyczka USB lub kamera HD lub kamera HD z kartą przechwytywania wideo - Dwurdzeniowy procesor 2 GHz lubszybszy(zalecany 4- rdzeniowy) (i3 / i5 / i7

lub odpowiednik AMD) - 2GB pamięci RAM (zalecane 4GB) - System operacyjny Windows 8(zalecanyWindows 10), Mac OS wersja

10.13 (zalecana najnowsza wersja) – dla PClub laptopa

Minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnik: - Stałe łącze

internetoweoprędkości 1,5 Mbps (zalecane2,5 Mbps z obrazem w jakości HD - 800kbps / 1.0Mbps (góra / dół) dla wysokiej jakości wideo

-Wprzypadku widoku galerii / lub video HD 720p: 1,5 / 1,5 (góra / dół) - Odbieranie wideo HD 1080p wymaga 2,5 (w górę / w dół) - Przesyłanie wideo HD1080pwymaga 3,0 (w górę / w dół) - Tylko do udostępniania ekranu (brak miniatury wideo): 50-75 - Doudostępniania ekranu z miniaturąwideo: 50-150 - W przypadku audio VoiP: 60-80 - W przypadku telefonu Zoom: 60-100

Niezbędne oprogramowanie umożliwiające Uczestnikom dostęp do prezentowanych treści i materiałów: -

Przeglądarka internetowa:Google Chrome, Firefox, lub Safari (zaktualizowane do najnowszej wersji) - Bezpłatna aplikacja „TEAMS" - Programy z możliwością odczytywania dokumentów„pdf”,„.doc”, „.xlsx”, ”.xls”, „.pptx”, „.

Podstawą do rozliczenia usługi, jest wygenerowanie z systemu raportu, umożliwiającego identyfikacjęwszystkich uczestników oraz zastosowanego narzędzia

Kontakt

Weronika Pasieba

E-mail projekty@posrednictwobiznesowe.pl
Telefon (+48) 530 163 879