Możliwość dofinansowania

AIBC SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

Brak ocen dla tego dostawcy

BEZPIECZEŃSTWO INFORMACJI I CYBERHIGIENA w miejscu pracy i w życiu prywatnym. Podstawowe pojęcia, przykłady ataków, dobre praktyki, reakcja na incydent.

Numer usługi 2026/04/03/195878/3464528

Usługa o charakterze zawodowym
zdalna w czasie rzeczywistym
03:00 h
05.06.2026 do 05.06.2026

369,00 PLN brutto
300,00 PLN netto
123,00 PLN brutto/h
100,00 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie skierowane jest do wszystkich osób aktywnych zawodowo, które w codziennej pracy lub życiu prywatnym korzystają z technologii informacyjno-komunikacyjnych oraz przetwarzają dane w formie cyfrowej. W szczególności do: 1. pracowników biurowych i administracyjnych 2. osób pracujących zdalnie lub hybrydowo 3. użytkowników komputerów, systemów IT i urządzeń mobilnych 4. osób przetwarzających dane osobowe, finansowe lub inne informacje wrażliwe 5. kadry zarządzającej i osób podejmujących decyzje operacyjne 6. wszystkich użytkowników poczty elektronicznej i narzędzi komunikacji online
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	50
Data zakończenia rekrutacji	04-06-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	3
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 jest podniesienie poziomu wiedzy i umiejętności uczestników w zakresie cyberbezpieczeństwa i cyberhigieny poprzez zapoznanie ich z podstawowymi pojęciami, najczęstszymi zagrożeniami oraz zasadami bezpiecznego korzystania z technologii informacyjno-komunikacyjnych w pracy i życiu prywatnym.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
rozpoznaje typowe zagrożenia cybernetyczne (m.in. phishing, socjotechnika, malware, ransomware, spoofing),	Walidacja efektów uczenia się zostanie przeprowadzona po zakończeniu szkolenia w formie: testu wiedzy.	Test teoretyczny
rozumie zasady bezpiecznego przetwarzania i ochrony danych,	Walidacja efektów uczenia się zostanie przeprowadzona po zakończeniu szkolenia w formie: testu wiedzy.	Test teoretyczny
stosuje dobre praktyki w zakresie korzystania z poczty elektronicznej, komunikatorów, haseł oraz urządzeń mobilnych	Walidacja efektów uczenia się zostanie przeprowadzona po zakończeniu szkolenia w formie: testu wiedzy.	Test teoretyczny
identyfikuje podejrzane sytuacje i próby wyłudzenia informacji,	Walidacja efektów uczenia się zostanie przeprowadzona po zakończeniu szkolenia w formie: testu wiedzy.	Test teoretyczny
potrafi właściwie zareagować na incydent bezpieczeństwa (izolacja, zgłoszenie, zabezpieczenie informacji),	Walidacja będzie odnosiła się bezpośrednio do efektów uczenia się określonych w Karcie Usługi. Warunkiem zaliczenia walidacji jest uzyskanie minimum 60% poprawnych odpowiedzi.	Test teoretyczny
kształtuje nawyki cyberhigieny ograniczające ryzyko naruszeń bezpieczeństwa informacji.	Walidacja efektów uczenia się zostanie przeprowadzona po zakończeniu szkolenia w formie: testu wiedzy.	Test teoretyczny

Kwalifikacje

Usługa o charakterze zawodowym

Kształcenie KKZ	A.35. - Planowanie i prowadzenie działalności w organizacji

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

09:00 – 09:45 (I moduł)

Wprowadzenie do cyberbezpieczeństwa i podstawowe zagrożenia

- Definicja cyberbezpieczeństwa i cyberhigieny
- Znaczenie bezpieczeństwa informacji w pracy i życiu prywatnym
- Podstawowe pojęcia: dane, incydent, malware, ransomware, phishing, spoofing
- Najczęstsze zagrożenia:
  - phishing (e-mail, SMS),
  - socjotechnika,
  - spoofing,
  - ataki telefoniczne (vishing)
- Przykłady realnych scenariuszy ataków

09:55 – 10:40 (II moduł)

Złośliwe oprogramowanie i nieautoryzowane pozyskiwanie danych

- Malware i ransomware – mechanizmy działania i skutki
- Metody nieautoryzowanego pozyskiwania danych:
  - wyłudzenia danych (phishing, spear phishing),
  - fałszywe strony i linki,
  - złośliwe załączniki,
  - przechwytywanie danych (np. keyloggery)
- Bezpieczne przetwarzanie danych:
  - szyfrowanie,
  - przechowywanie danych,
  - zasady udostępniania informacji
- Dobre praktyki w codziennej pracy

10:50 – 11:35 (III moduł)

Bezpieczna komunikacja i reagowanie na incydenty

- Bezpieczna komunikacja:

    - e-mail, komunikatory, linki i załączniki
- Social media i urządzenia mobilne – zagrożenia i zasady bezpieczeństwa
- Reakcja na incydent:
    - identyfikacja zagrożenia,
    - izolacja problemu,
    - zgłoszenie incydentu,
    - zabezpieczenie informacji
- Gdzie zgłaszać incydenty (procedury organizacyjne, CSIRT)
- Podsumowanie i najważniejsze zasady cyberhigieny

11:35 – 12:00 (walidacja efektów uczenia się)

Forma walidacji:

- test wiedzy (zamknięty, jednokrotnego wyboru),
- krótkie studium przypadku / scenariusz sytuacyjny,

Zakres walidacji:

- rozpoznawanie zagrożeń (phishing, malware, socjotechnika),
- zasady bezpiecznej pracy z informacją,
- reakcja na incydent.

Harmonogram

Liczba pozycji harmonogramu: 4

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 4 Wprowadzenie do cyberbezpieczeństwa i podstawowe zagrożenia	-	05-06-2026	09:00	09:45	00:45
2 z 4 Złośliwe oprogramowanie i nieautoryzowane pozyskiwanie danych	-	05-06-2026	09:55	10:40	00:45
3 z 4 Bezpieczna komunikacja i reagowanie na incydenty	-	05-06-2026	10:50	11:35	00:45
4 z 4 Walidacja efektów uczenia się	-	05-06-2026	11:35	12:00	00:25

Cennik

Jeżeli korzystasz z dofinansowania w wysokości co najmniej 70% przysługuje Tobie zwolnienie z podatku VAT

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	369,00 PLN
Koszt przypadający na 1 uczestnika netto	300,00 PLN
Koszt osobogodziny brutto	123,00 PLN
Koszt osobogodziny netto	100,00 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymają materiały szkoleniowe w formie elektronicznej, obejmujące:

- prezentację szkoleniową,
- praktyczne zasady tworzenia silnych haseł.

Warunki uczestnictwa

Uczestnik powinien posiadać:

1. komputer, laptop lub tablet z dostępem do Internetu
2. stabilne łącze internetowe (minimum 5 Mb/s)
3. przeglądarkę internetową (np. Google Chrome, Edge, Firefox)
4. działający mikrofon, opcjonalnie kamera internetowa

Zalecane: korzystanie ze słuchawek w celu poprawy jakości dźwięku

Warunki techniczne

Organizator zapewnia:

realizację szkolenia na platformie

Google Meet, umożliwiającej:

- transmisję audio i wideo w czasie rzeczywistym
- udostępnianie ekranu
- komunikację przez czat
- interakcję z uczestnikami (pytania, dyskusja)
- dostęp do spotkania przez cały czas trwania szkolenia (link aktywny przez cały czas szkolenia)
- prowadzenie szkolenia przez wykwalifikowanego trenera
- wsparcie techniczne w trakcie szkolenia (w razie problemów z dołączeniem)
- możliwość potwierdzenia obecności uczestników (np. lista obecności, raporty z Google Meet)

Kontakt

MAŁGORZATA MICHNIEWICZ

E-mail michniewicz2010@gmail.com

Telefon (+48) 662 013 215