



Gdela Krystyna
AKUSTICA.MED

★★★★★ 4,9 / 5

921 ocen

Cyberbezpieczeństwo w branży ubezpieczeniowej

Numer usługi 2025/09/08/22012/2991305

📍 Janów Podlaski / stacjonarna

🏠 Usługa szkoleniowa

🕒 16 h

📅 20.09.2025 do 21.09.2025

4 214,00 PLN brutto

4 214,00 PLN netto

263,38 PLN brutto/h

263,38 PLN netto/h

Informacje podstawowe

Kategoria	Finanse i bankowość / Ubezpieczenia
Grupa docelowa usługi	• Doradcy ubezpieczeniowi • Menadżerowie sprzedaży • Liderzy zespołów • Doświadczeni agenci/doradcy • Nowi agenci ubezpieczeniowi
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	25
Data zakończenia rekrutacji	19-09-2025
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	16
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

1. Zwiększenie świadomości zagrożeń cybernetycznych
2. Poznanie przepisów i regulacji dotyczących ochrony danych
3. Nabycie umiejętności reagowania na incydenty
4. Zrozumienie roli każdego pracownika w systemie bezpieczeństwa informacji
5. Identyfikacja i minimalizacja ryzyk w pracy codziennej

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Potrafi rozpoznawać podejrzane wiadomości i próby wyludzenia danych (np. phishing, spear phishing)	Poprawnie klasyfikuje przykłady wiadomości jako „bezpieczne” lub „podejrzane”	Obserwacja w warunkach symulowanych
Potrafi bezpiecznie korzystać z narzędzi cyfrowych – aplikacji ubezpieczeniowych, poczty e-mail, systemów CRM	Loguje się do aplikacji/systemu z użyciem silnego hasła lub MFA (multi-factor authentication)	Obserwacja w warunkach symulowanych
Potrafi stosować zasady bezpiecznego przetwarzania danych osobowych klientów	Rozpoznaje naruszenia ochrony danych osobowych w scenariuszach (np. ujawnienie danych przez e-mail)	Obserwacja w warunkach symulowanych
Potrafi zgłaszać incydenty zgodnie z procedurami firmy oraz wiedzieć, do kogo się zgłosić w razie problemu	Wymienia właściwą osobę / dział do kontaktu w razie incydentu (np. dział bezpieczeństwa IT, inspektor ochrony danych)	Obserwacja w warunkach symulowanych
Potrafi unikać błędów, które mogą prowadzić do naruszeń bezpieczeństwa (np. korzystanie z niezabezpieczonych sieci Wi-Fi, zapisywanie haseł w niebezpieczny sposób)	Wskazuje poprawne i niepoprawne praktyki z zakresu bezpieczeństwa IT (np. quiz wyboru, gra decyzyjna)	Obserwacja w warunkach symulowanych

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

Program szkolenia: „Cyberbezpieczeństwo w branży ubezpieczeniowej” (16 godzin)

Dzień 1 (8 godzin)

1. Wprowadzenie do cyberbezpieczeństwa (1,5h)

- Czym jest cyberbezpieczeństwo?
- Aktualne trendy zagrożeń w branży ubezpieczeniowej
- Przykłady rzeczywistych incydentów w sektorze finansowym

2. Zagrożenia cybernetyczne – identyfikacja i przykłady (1,5h)

- Phishing, spear phishing, smishing, vishing
- Ransomware, malware, keyloggers
- Ataki DDoS, spoofing, socjotechnika
- Ćwiczenia: analiza fałszywych e-maili

3. Bezpieczne przetwarzanie danych osobowych i regulacje prawne (1,5h)

- RODO – obowiązki i zasady
- Rekomendacje KNF dotyczące bezpieczeństwa informacji
- Ustawa o krajowym systemie cyberbezpieczeństwa
- Obowiązki firm ubezpieczeniowych jako administratorów danych

4. Rola użytkownika końcowego w systemie bezpieczeństwa (1,5h)

- Dlaczego każdy pracownik jest potencjalnym celem
- Bezpieczna praca na komputerze i zdalnie
- Przykłady codziennych zagrożeń i dobrych praktyk

Dzień 2 (8 godzin)

6. Zabezpieczanie danych i systemów – dobre praktyki (1,5h)

- Hasła, uwierzytelnianie dwuskładnikowe
- Bezpieczne korzystanie z poczty, internetu i nośników danych
- Szyfrowanie danych i kopie zapasowe

7. Incydenty bezpieczeństwa – procedury reagowania i zgłaszania (1,5h)

- Co to jest incydent bezpieczeństwa?
- Etapy reagowania na incydent
- Rola Działu IT, ABI/Inspektora Ochrony Danych
- Zgłaszanie naruszeń do UODO / KNF

8. Audyty, kontrole i compliance (1,5 h)

- Wewnętrzne procedury kontroli
- Jak wygląda audyt cyberbezpieczeństwa?
- Jak przygotować się do kontroli regulatora?

9. Przyszłość cyber-zagrożeń – jak się przygotować? (1h 15 min)

- Nowe technologie i ich ryzyka (AI, IoT, chmura)
- Cyberpolisy – ubezpieczenie od ryzyk cyfrowych
- Budowanie kultury cyberbezpieczeństwa w firmie

10. Walidacja efektów uczenia się (15 min)

Harmonogram

Liczba przedmiotów/zajęć: 15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 15 Wprowadzenie do cyberbezpieczeństwa	Beniamin Sosidko	20-09-2025	09:00	10:30	01:30
2 z 15 Przerwa kawowa	Beniamin Sosidko	20-09-2025	10:30	10:45	00:15
3 z 15 Zagrożenia cybernetyczne – identyfikacja i przykłady	Beniamin Sosidko	20-09-2025	10:45	12:15	01:30
4 z 15 Przerwa obiadowa	Beniamin Sosidko	20-09-2025	12:15	12:45	00:30
5 z 15 Bezpieczne przetwarzanie danych osobowych i regulacje prawne	Beniamin Sosidko	20-09-2025	12:45	14:15	01:30
6 z 15 Przerwa kawowa	Beniamin Sosidko	20-09-2025	14:15	14:30	00:15
7 z 15 Rola użytkownika końcowego w systemie bezpieczeństwa	Beniamin Sosidko	20-09-2025	14:30	16:00	01:30
8 z 15 Zabezpieczanie danych i systemów – dobre praktyk	Beniamin Sosidko	21-09-2025	09:00	10:30	01:30
9 z 15 Przerwa kawowa	Beniamin Sosidko	21-09-2025	10:30	10:45	00:15
10 z 15 Incydenty bezpieczeństwa – procedury reagowania i zgłaszania	Beniamin Sosidko	21-09-2025	10:45	12:15	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
11 z 15 Przerwa obiadowa	Beniamin Sosidko	21-09-2025	12:15	12:45	00:30
12 z 15 Audyty, kontrole i compliance	Beniamin Sosidko	21-09-2025	12:45	14:15	01:30
13 z 15 Przerwa kawowa	Beniamin Sosidko	21-09-2025	14:15	14:30	00:15
14 z 15 Przyszłość cyberzagrożeń – jak się przygotować?	Beniamin Sosidko	21-09-2025	14:30	15:45	01:15
15 z 15 Walidacja efektów uczenia się	-	21-09-2025	15:45	16:00	00:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 214,00 PLN
Koszt przypadający na 1 uczestnika netto	4 214,00 PLN
Koszt osobogodziny brutto	263,38 PLN
Koszt osobogodziny netto	263,38 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Beniamin Sosidko

Ukończone studia inżynierskie na kierunku Informatyka o specjalizacji: Inżynieria oprogramowania i systemów sieciowych. Ukończone szkolenia i kursy:
ITIL Foundation with ITIL Foundation Certificate in IT Service Managment organizowane przez Altkom

Akademia,
COBIT 5 Fundation Certificate organizowane przez Inprogress,
Wykorzystanie Chat GPT w Pracy Biurowej i Marketingu,
ChatGPT: Generowanie i Wykorzystanie AI.
Jak trener przeprowadził szkolenia komputerowe zgodnie z ramą DigCOMP w łącznej liczbie 932 godzin.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Informacje o materiałach dla uczestników usługi

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymują:

Gotowe szablony poleceń.

Certyfikat Uczestnictwa w szkoleniu.

Szkolenie prowadzone jest w formie godzin dydaktycznych 1h= 45min

Metodyka szkolenia: Szkolenie odbywa się w formie warsztatów.

Usługa zwolniona jest z podatku VAT jeśli przedsiębiorca uzyskuje min. 70% dofinansowania ze środków publicznych*, w przeciwnym wypadku należy do ceny netto doliczyć 23% VAT. *Wg rozporządzenia Ministra Finansów z dnia z dnia 20.12.2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (Dz. U. z 2018, poz. 701)//.

Adres

ul. Zamkowa 1
21-505 Janów Podlaski
woj. lubelskie

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Laboratorium komputerowe

Kontakt



Robert Gdela

E-mail biuro@akusticamed.com

Telefon (+48) 793 793 990