



Zaawansowane Strategie Cyberbezpieczeństwa i Zarządzania Ryzykiem w Środowisku Cyfrowym

Numer usługi 2025/03/25/180138/2647786

5 320,00 PLN brutto

5 320,00 PLN netto

133,00 PLN brutto/h

133,00 PLN netto/h

HC SPÓŁKA Z
OGRANICZONĄ
ODPOWIEDZIALNOŚĆ
CIA



📍 zdalna w czasie rzeczywistym

👤 Usługa szkoleniowa

🕒 40 h

📅 19.05.2025 do 22.05.2025

Informacje podstawowe

Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

Sposób dofinansowania

wsparcie dla osób indywidualnych
wsparcie dla pracodawców i ich pracowników

Grupa docelowa usługi

Szkolenie skierowane jest do:

1. Pracowników Firm i Instytucji

- Osoby zatrudnione w działach administracji, kadr, marketingu czy innych obszarach, które w codziennych obowiązkach korzystają z urządzeń elektronicznych i internetu.

2. Managerów i Kadr Zarządzających

- Osoby odpowiedzialne za polityki bezpieczeństwa danych w firmie, procedury wewnętrzne oraz zarządzanie ryzykiem cybernetycznym.

3. Specjalistów IT i Pracowników Działów Technicznych

- Osoby techniczne, które chcą usystematyzować swoją wiedzę, pogłębić kompetencje oraz wdrożyć skuteczne zabezpieczenia w organizacjach.

4. Osoby Odpowiedzialne za Zgodność Prawną (Compliance/Inspektorzy Ochrony Danych/RODO)

- Specjaliści zajmujący się realizacją wymogów prawnych związanych z ochroną danych osobowych i cyberbezpieczeństwem.

5. Użytkownicy Internetu na Codzień

- Każda osoba, która chce chronić swoją tożsamość, finanse i prywatność w sieci, niezależnie od swojego poziomu zaawansowania technicznego.

Minimalna liczba uczestników

1

Maksymalna liczba uczestników

15

Data zakończenia rekrutacji	18-05-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	40
Podstawa uzyskania wpisu do BUR	Znak Jakości TGLS Quality Alliance

Cel

Cel edukacyjny

Szkolenie skupia się na rozwijaniu kompetencji w zakresie cyberbezpieczeństwa oraz zarządzania ryzykiem w środowisku cyfrowym. Uczestnicy zdobywają praktyczne umiejętności w stosowaniu najnowszych standardów ochrony danych, technik szyfrowania, autoryzacji dwuetapowej oraz procedur reagowania na ataki cybernetyczne.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Określenie kluczowych pojęć związanych z cyberbezpieczeństwem, takich jak malware, phishing, szyfrowanie danych.	Uczestnik poprawnie definiuje terminy związane z cyberbezpieczeństwem.	Test teoretyczny z wynikiem generowanym automatycznie
Klasyfikacja typów zagrożeń cyfrowych i metody ich rozpoznawania.	Uczestnik rozróżnia rodzaje zagrożeń cyfrowych.	Test teoretyczny z wynikiem generowanym automatycznie
Wyjaśnienie znaczenia aktualizacji oprogramowania dla bezpieczeństwa systemów	Uczestnik opisuje konsekwencje nieaktualizacji oprogramowania	Test teoretyczny z wynikiem generowanym automatycznie
Demonstracja tworzenia i zarządzania bezpiecznymi hasłami	Uczestnik stosuje zasady silnych haseł w praktyce	Test teoretyczny z wynikiem generowanym automatycznie
Identyfikacja próbek phishingu i reagowanie na oszustwa internetowe	Uczestnik identyfikuje fałszywe wiadomości e-mail i strony internetowe.	Test teoretyczny z wynikiem generowanym automatycznie
Krytyczna ocena informacji w Internecie.	Uczestnik analizuje wiarygodność źródeł danych.	Test teoretyczny z wynikiem generowanym automatycznie
Interpretacja przepisów prawa w zakresie ochrony danych osobowych i cyberbezpieczeństwa	Uczestnik wyjaśnia zastosowanie przepisów RODO w praktyce	Test teoretyczny z wynikiem generowanym automatycznie
Stworzenie kopii zapasowych plików i zarządzanie nimi.	Uczestnik organizuje proces backupu danych	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Implementacja autoryzacji dwuetapowej w mediach społecznościowych	Uczestnik aktywuje dwuskładnikową autoryzację.	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

Tak, dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się.

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

Tak, dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji.

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

Tak, dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji.

Program

Program Szkolenia

Dzień Pierwszy: Fundamenty Cyberbezpieczeństwa

- Wprowadzenie do cyberbezpieczeństwa:
 - Definicja i podstawowe terminy.
 - Podstawy prawne cyberbezpieczeństwa.
- Najpopularniejsze ataki cybernetyczne:
 - Phishing i inne formy oszustw.
 - Praktyczne ćwiczenia.

Dzień Drugi: Ochrona Danych i Autoryzacja

- Przestępstwa finansowe w przestrzeni cyfrowej.
- Zarządzanie hasłami:
 - Standardy bezpieczeństwa.
 - Wybór menedżera haseł.
- Zabezpieczenia przed cyberatakami:
 - Autoryzacja dwuetapowa.
 - Szyfrowanie danych.

Dzień Trzeci: Zabezpieczenia Systemowe

1. Backup danych:
 - Skuteczne strategie tworzenia kopii zapasowych.
2. Ochrona sprzętu i prywatności:
 - Antywirusy, firewally, tryb incognito.
 - Socjotechniki wykorzystywane przez hakerów.
3. Prawne aspekty cyberbezpieczeństwa:
 - Regulacje RODO.

Dzień Czwarty: Aktualne Zagrożenia i Reakcje

1. Fake newsy i narzędzia AI:
 - Mechanizmy generowania fałszywych treści.
2. Legalne metody pozyskiwania danych (OSINT).
3. Procedury reagowania na ataki cybernetyczne:
 - Formalne i komunikacyjne kroki.
4. Podsumowanie
5. Test teoretyczny z wynikiem generowanym automatycznie - walidacja

Szkolenie odbywa się w godzinach dydaktycznych, czyli 1 godzina szkolenia równa się 45 minut, łącznie 40 godzin dydaktycznych.

Prowadzone w ramach szkolenia zajęcia realizowane są metodami interaktywnymi i aktywizującymi, rozumianymi jako metody umożliwia

Po 90 minutach szkolenia przewidziana jest przerwa kawowa 15min

Harmonogram

Liczba przedmiotów/zajęć: 12

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 12 Wprowadzenie do cyberbezpieczeństwa	Joanna Dubisz	19-05-2025	08:00	12:00	04:00
2 z 12 Najpopularniejsze ataki cybernetyczne	Joanna Dubisz	19-05-2025	12:00	16:00	04:00
3 z 12 Przestępstwa finansowe w przestrzeni cyfrowej	Joanna Dubisz	20-05-2025	08:00	11:00	03:00
4 z 12 Zarządzanie hasłami	Joanna Dubisz	20-05-2025	11:00	13:00	02:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 12 Zabezpieczenia przed cyberatakami	Joanna Dubisz	20-05-2025	13:00	15:00	02:00
6 z 12 Backup danych	Joanna Dubisz	21-05-2025	08:00	10:00	02:00
7 z 12 Ochrona sprzętu i prywatności	Joanna Dubisz	21-05-2025	10:00	13:00	03:00
8 z 12 Prawne aspekty cyberbezpieczeństwa	Joanna Dubisz	21-05-2025	13:00	15:00	02:00
9 z 12 Fake newsy i narzędzia AI	Joanna Dubisz	22-05-2025	08:00	11:00	03:00
10 z 12 Legalne metody pozyskiwania danych (OSINT)	Joanna Dubisz	22-05-2025	11:00	13:00	02:00
11 z 12 Procedury reagowania na ataki cybernetyczne	Joanna Dubisz	22-05-2025	13:00	15:00	02:00
12 z 12 Test teoretyczny z wynikiem generowanym automatycznie - walidacja	Joanna Dubisz	22-05-2025	15:00	16:00	01:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 320,00 PLN
Koszt przypadający na 1 uczestnika netto	5 320,00 PLN

Koszt osobogodziny brutto	133,00 PLN
---------------------------	------------

Koszt osobogodziny netto	133,00 PLN
--------------------------	------------

Prowadzący

Liczba prowadzących: 1



1 z 1

Joanna Dubisz

Joanna Dubisz to doświadczona szkoleniowiczka specjalizująca się w obszarach sprzedaży oraz obsługi klienta. Swoją edukację rozpoczęła od ukończenia liceum profilowanego o kierunku socjalnym, co dało jej solidne podstawy w zakresie pracy z ludźmi i zrozumienia ich potrzeb. Karierę szkoleniowiczki rozpoczęła w 2018 roku i od tego czasu nieustannie rozwija swoje umiejętności, zdobywając liczne certyfikaty, w tym z zakresu pracy w zespole oraz radzenia sobie z trudnymi klientami.

Joanna zrealizowała ponad 300 godzin szkoleń, prowadząc warsztaty zarówno dla firm, jak i klientów indywidualnych. Jej szkolenia cechują się praktycznym podejściem i są dostosowane do rzeczywistych potrzeb uczestników, dzięki czemu potrafi efektywnie przekazywać wiedzę, jednocześnie budując zaangażowanie i motywację w zespole. Dzięki swojemu doświadczeniu oraz umiejętnościom w zarządzaniu relacjami z klientem, Joanna cieszy się opinią eksperta w zakresie rozwijania kompetencji sprzedażowych i obsługi klienta."

Joanna jest specjalistką do spraw zarządzania cyberbezpieczeństwem w firmach.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Komplet materiałów zostanie wysłany w wiadomości e-mail dla każdego z uczestników szkolenia.

Zestaw materiałów szkoleniowych składa się z prezentacji oraz skryptu szkolenia.

Informacje dodatkowe

Uczestnik szkolenia otrzyma zaświadczenie o ukończeniu szkolenia dopiero po pozytywnym wyniku walidacji, która składa się z testu sprawdz

Szkolenie jest zwolnione z podatku VAT na podstawie §3 ust.1 pkt 14 rozporządzenia Ministra Finansów z dnia 20.12.2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (Dz.U. z 2015 r., poz.736)).

Jeśli dofinansowanie za szkolenie ze środków publicznych wyniesie poniżej 70%, do kwoty faktury zostanie doliczona stawka podatku VAT (23%).

Do wybranej metody walidacji nie jest potrzebny walidator, ponieważ uczestnicy dostają link do wypełnienia testu

Warunki techniczne

1. Platforma komunikacyjna – Microsoft Teams
2. Wymagania sprzętowe: komputer stacjonarny/laptop, kamera, mikrofon, słuchawki/ głośniki, system operacyjny minimum Windows XP/Mac
3. Sieć: łącze internetowe minimum 50 kb/s;
4. System operacyjny: minimum Windows XP/MacOS High Sierra, przeglądarka internetowa (marka nie ma znaczenia)
5. Okres ważności linku: od 1 h przed godziną rozpoczęcia szkolenia w dniu pierwszym do godziny po zakończeniu szkoleń w dniu ostatnim.

Kontakt



Jakub Mencfeld

E-mail szkolenia@hameracapital.eu

Telefon (+48) 661 336 370