Możliwość dofinansowania

Cyberbezpieczeństwo — usługa szkoleniowa

Numer usługi 2025/12/11/180138/3207078

5 400,00 PLN brutto
5 400,00 PLN netto
135,00 PLN brutto/h
135,00 PLN netto/h

HC SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

4,9 / 5

978 ocen

Kołobrzeg / stacjonarna
Usługa szkoleniowa
40 h
19.01.2026 do 23.01.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	• pracownicy i/lub właściciele pracujący z komputerem, Internetem oraz urządzeniami mobilnymi • pracownicy z sektora MSP **Szkolenie jest przeznaczone przede wszystkim dla osób chcących chronić dane firmy, rozpoznawać oszustwa np. w mediach społecznościowych oraz odpowiednio reagować na nie.**
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	18-01-2026
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	40
Podstawa uzyskania wpisu do BUR	Znak Jakości TGLS Quality Alliance

Cel

Cel edukacyjny

Usługa ma na celu zwiększenie świadomości i kompetencji uczestników w zakresie cyberbezpieczeństwa oraz higieny w sieci, z naciskiem na rozumienie i praktyczne stosowanie najlepszych praktyk i strategii obrony przed zagrożeniami cybernetycznymi w środowisku zawodowym i osobistym.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Omawia podstawowe pojęcia związane z cyberbezpieczeństwem i higieną w sieci, takie jak malware, phishing, bezpieczne hasła i szyfrowanie danych.	Uczestnik poprawnie definiuje wymienione pojęcia i opisuje ich znaczenie w kontekście bezpieczeństwa sieciowego.	Obserwacja w warunkach symulowanych
Charakteryzuje różne typy zagrożeń cyfrowych oraz metody ich rozpoznawania.	Uczestnik wymienia i opisuje co najmniej trzy różne typy zagrożeń, podając przykłady oraz sposoby ich identyfikacji.	Test teoretyczny
Definiuje znaczenie aktualizacji oprogramowania w kontekście zabezpieczeń cyfrowych.	Uczestnik wyjaśnia, dlaczego regularne aktualizacje oprogramowania są kluczowe dla zachowania bezpieczeństwa systemów i danych.	Test teoretyczny
Stosuje praktyki tworzenia i zarządzania bezpiecznymi hasłami.	Uczestnik demonstruje umiejętność tworzenia silnych haseł i korzystania z menedżerów haseł do ich przechowywania.	Obserwacja w warunkach symulowanych
Identyfikuje i reaguj na próby phishingu i inne oszustwa internetowe.	Uczestnik poprawnie identyfikuje fałszywe wiadomości e-mail i strony internetowe oraz zna procedury reagowania na te zagrożenia.	Test teoretyczny
Stosuje zasady bezpiecznego korzystania z sieci publicznych i prywatnych.	Uczestnik potrafi skonfigurować bezpieczne połączenie sieciowe i stosuje praktyki ochrony prywatności podczas korzystania z sieci publicznych.	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

Dzień 1:

1. wprowadzenie do szkolenia
2. audyt cyberbezpieczeństwa
3. istota i podstawowe terminy w zakresie cyberbezpieczeństwa
4. podstawy prawne cyberbezpieczeństwa i zalecenia ENISA
5. najpopularniejsze ataki cybernetyczne

Dzień 2:

1. ćwiczenie: phishing
2. przestępstwa finansowe w przestrzeni cyfrowej
3. zasady ustalania haseł zgodnie z obecnymi standardami bezpieczeństwa cyfrowego
4. jak działa i jak wybrać menadżera haseł?
5. dlaczego tak często hakerzy łamią hasła?

Dzień 3:

1. dlaczego samo hasło nie wystarczy? Autoryzacja dwuskładnikowa w praktyce
2. szyfrowanie plików,folderów i pendrive'ów w praktyce
3. jak chronić dane osobowe zgodnie z RODO?
4. zastrzeż swój PESEL
5. jak robić backup danych?

Dzień 4:

1. dlaczego warto korzystać z„chmury”?
2. wykorzystywanie AI przez cyberprzestępców – jak nie dać się nabrać?
3. jak zabezpieczyć swój sprzęt i prywatność? Programy antywirusowe, firewall, tryb incognito, cookies, VPN
4. co o nas wiedzą? - socjotechniki wykorzystywane przez hakerów
5. co zrobić, gdy zostanę zaatakowany? Procedura formalna i komunikacyjna

Dzień 5:

1. jak wzmocnić kulturę cyberbezpieczeństwa w organizacji?
2. jak rodzą się fake newsy przez wykorzystywanie narzędzi AI?
3. ćwiczenie grupowe: symulacje ataków cybernetycznych
4. narzędzia i programy wzmacniające bezpieczeństwo cyfrowe
5. Podsumowanie
6. Walidacja

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

Przerwy ujęte w harmonogramie nie są wliczane w czas trwania szkolenia.

Prowadzone w ramach szkolenia zajęcia realizowane są metodami interaktywnymi i aktywizującymi, rozumianymi jako metody umożliwiające uczenie się w oparciu o doświadczenie i pozwalające uczestnikom na ćwiczenie umiejętności.

Harmonogram

Liczba przedmiotów/zajęć: 36

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 36 wprowadzenie do szkolenia	Joanna Mikołajczyk	19-01-2026	08:00	09:00	01:00
2 z 36 audyt cyberbezpieczeństwa	Joanna Mikołajczyk	19-01-2026	09:00	10:00	01:00
3 z 36 Przerwa	Joanna Mikołajczyk	19-01-2026	10:00	10:30	00:30
4 z 36 istota i podstawowe terminy w zakresie cyberbezpieczeństwa	Joanna Mikołajczyk	19-01-2026	10:30	11:30	01:00
5 z 36 podstawy prawne cyberbezpieczeństwa i zalecenia ENISA	Joanna Mikołajczyk	19-01-2026	11:30	12:30	01:00
6 z 36 Przerwa	Joanna Mikołajczyk	19-01-2026	12:30	13:00	00:30
7 z 36 najpopularniejsze ataki cybernetyczne	Joanna Mikołajczyk	19-01-2026	13:00	15:00	02:00
8 z 36 ćwiczenie: phishing	Joanna Mikołajczyk	20-01-2026	08:00	09:00	01:00
9 z 36 przestępstwa finansowe w przestrzeni cyfrowej	Joanna Mikołajczyk	20-01-2026	09:00	10:00	01:00
10 z 36 Przerwa	Joanna Mikołajczyk	20-01-2026	10:00	10:30	00:30
11 z 36 zasady ustalania haseł zgodnie z obecnymi standardami bezpieczeństwa cyfrowego	Joanna Mikołajczyk	20-01-2026	10:30	11:30	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
12 z 36 jak działa i jak wybrać menadżera haseł?	Joanna Mikołajczyk	20-01-2026	11:30	12:30	01:00
13 z 36 Przerwa	Joanna Mikołajczyk	20-01-2026	12:30	13:00	00:30
14 z 36 dlaczego tak często hakerzy łamią hasła?	Joanna Mikołajczyk	20-01-2026	13:00	15:00	02:00
15 z 36 dlaczego samo hasło nie wystarczy? Autoryzacja dwuskładnikowa w praktyce	Joanna Mikołajczyk	21-01-2026	08:00	09:00	01:00
16 z 36 szyfrowanie plików,folderów i pendrive'ów w praktyce	Joanna Mikołajczyk	21-01-2026	09:00	10:00	01:00
17 z 36 Przerwa	Joanna Mikołajczyk	21-01-2026	10:00	10:30	00:30
18 z 36 jak chronić dane osobowe zgodnie z RODO?	Joanna Mikołajczyk	21-01-2026	10:30	11:30	01:00
19 z 36 zastrzeż swój PESEL	Joanna Mikołajczyk	21-01-2026	11:30	12:30	01:00
20 z 36 Przerwa	Joanna Mikołajczyk	21-01-2026	12:30	13:00	00:30
21 z 36 jak robić backup danych?	Joanna Mikołajczyk	21-01-2026	13:00	15:00	02:00
22 z 36 dlaczego warto korzystać z„chmury”?	Joanna Mikołajczyk	22-01-2026	08:00	09:00	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
23 z 36 wykorzystywanie AI przez cyberprzestępców – jak nie dać się nabrać?	Joanna Mikołajczyk	22-01-2026	09:00	10:00	01:00
24 z 36 Przerwa	Joanna Mikołajczyk	22-01-2026	10:00	10:30	00:30
25 z 36 jak zabezpieczyć swój sprzęt i prywatność? Programy antywirusowe, firewall, tryb incognito, cookies, VPN	Joanna Mikołajczyk	22-01-2026	10:30	11:30	01:00
26 z 36 co o nas wiedzą? - socjotechniki wykorzystywane przez hakerów	Joanna Mikołajczyk	22-01-2026	11:30	12:30	01:00
27 z 36 Przerwa	Joanna Mikołajczyk	22-01-2026	12:30	13:00	00:30
28 z 36 co zrobić, gdy zostanę zaatakowany? Procedura formalna i komunikacyjna	Joanna Mikołajczyk	22-01-2026	13:00	15:00	02:00
29 z 36 jak wzmocnić kulturę cyberbezpieczeństwa w organizacji?	Joanna Mikołajczyk	23-01-2026	08:00	09:00	01:00
30 z 36 jak rodzą się fake newsy przez wykorzystywanie narzędzi AI?	Joanna Mikołajczyk	23-01-2026	09:00	10:00	01:00
31 z 36 Przerwa	Joanna Mikołajczyk	23-01-2026	10:00	10:30	00:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
32 z 36 ćwiczenie grupowe: symulacje ataków cybernetycznych	Joanna Mikołajczyk	23-01-2026	10:30	11:30	01:00
33 z 36 narzędzia i programy wzmacniające bezpieczeństwo cyfrowe	Joanna Mikołajczyk	23-01-2026	11:30	12:30	01:00
34 z 36 Przerwa	Joanna Mikołajczyk	23-01-2026	12:30	13:00	00:30
35 z 36 Podsumowanie	Joanna Mikołajczyk	23-01-2026	13:00	14:00	01:00
36 z 36 Test wiedzy - walidacja	-	23-01-2026	14:00	15:00	01:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 400,00 PLN
Koszt przypadający na 1 uczestnika netto	5 400,00 PLN
Koszt osobogodziny brutto	135,00 PLN
Koszt osobogodziny netto	135,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Joanna Mikołajczyk

Jestem pedagogiem socjalnym z pasją do pracy z ludźmi i rozwijania ich potencjału. Jako coach i mentor skutecznie wspieram innych w osiąganiu celów. Specjalizuję się w profilaktyce społecznej

oraz prowadzeniu szkoleń z zakresu skutecznej sprzedaży, obsługi trudnego klienta, zarządzania procesami i budowania zespołów.

Obecnie pracuję jako szkoleniowiec w Vantis Holding, gdzie opracowuję i realizuję programy szkoleniowe dostosowane do potrzeb uczestników. Mam także duże doświadczenie w walidacji szkoleń z różnych obszarów, co pozwala mi dbać o ich wysoką jakość, merytorykę i skuteczność.

Jestem certyfikowanym trenerem w Vantis Holding, co potwierdza moje kompetencje w zakresie prowadzenia szkoleń oraz technik sprzedaży i zarządzania. Posiadam doskonałe umiejętności komunikacyjne, zdolności coachingowe oraz szeroką wiedzę z obszaru HR i sprzedaży. Moim celem jest inspirowanie i rozwijanie potencjału ludzi poprzez praktyczne i angażujące szkolenia oraz zapewnianie ich najwyższego standardu poprzez proces walidacji.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały zostaną przesłane drogą mailową w formacie pdf. Uczestnik otrzyma:

1. skrypty

2. materiały video

Informacje dodatkowe

Szkolenie przeznaczone jest dla pracowników firmy INVEST TOWER

Adres

ul. Budowlana 6
78-100 Kołobrzeg
woj. zachodniopomorskie

Szkolenie odbywać się będzie w "Restauracja i Browar Colberg" w przypadku problemów z dotarciem proszę o kontakt telefoniczny 888 677 422

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi

Kontakt

DOMINIK HAMERA

E-mail office@hameracapital.eu
Telefon (+48) 888 677 422