Możliwość dofinansowania

Bezpieczna transformacja cyfrowa: Cyberochrona przedsiębiorstwa na poziomie międzynarodowym – zagrożenia, prawo, odporność

Numer usługi 2025/05/23/153767/2766583

6 375,00 PLN brutto
6 375,00 PLN netto
255,00 PLN brutto/h
255,00 PLN netto/h

K2 CONSULTING SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

★★★★★

Puławy / stacjonarna
Usługa szkoleniowa
25 h
03.07.2025 do 05.07.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Szkolenie skierowane jest do pracowników, którzy niezależnie od zajmowanych stanowisk, w swojej codziennej pracy korzystają z infrastruktury IT, systemów informatycznych lub mają dostęp do danych firmowych. Uczestnicy nie muszą posiadać specjalistycznej wiedzy technicznej, ale powinni rozumieć znaczenie bezpiecznego korzystania z narzędzi cyfrowych w środowisku zawodowym. Wymagany jest minimalny staż pracy wynoszący 1 miesiąc.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	11
Data zakończenia rekrutacji	02-07-2025
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	25
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 świadomości uczestników w zakresie cyberzagrożeń oraz przekazanie praktycznej wiedzy i umiejętności niezbędnych do bezpiecznego korzystania z technologii cyfrowych w pracy. Uczestnicy nauczą się rozpoznawać potencjalne zagrożenia, reagować na incydenty oraz stosować podstawowe zasady ochrony danych i systemów informatycznych, zgodnie z aktualnymi wymogami prawnymi i dobrymi praktykami.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik definiuje cel transformacji cyfrowej w przedsiębiorstwach	Podaje i opisuje przynajmniej 2 proste przykłady działań cyfryzacyjnych w firmie (np. e-faktury, praca zdalna, automatyzacja procesów)	Wywiad swobodny
Uczestnik rozpoznaje podstawowe zagrożenia cyfryzacji	Opisuje krótko przykład jednego realnego incydentu (z życia lub omawianego na szkoleniu)	Wywiad swobodny
Uczestnik wyjaśnia znaczenie cyberbezpieczeństwa dla firmy	Wskazuje skutki ataku na firmę (np. straty finansowe, przestój, utrata zaufania)	Wywiad swobodny
Uczestnik opisuje przebieg typowego cyberataku i sposoby jego rozpoznania	Wymienia etapy ataku (np. podejrzany mail → kliknięcie → infekcja)	Wywiad swobodny
Uczestnik wskazuje dobre praktyki zabezpieczania się przed cyberzagrożeniami	Podaje co najmniej 3 działania ochronne (np. silne hasła, kopie zapasowe, aktualizacje)	Wywiad swobodny
Uczestnik wymienia podstawowe obowiązki firmy wynikające z przepisów	Podaje przykład sankcji lub kontroli w razie zaniedbań	Wywiad swobodny
Uczestnik rozpoznaje elementy podstawowej polityki bezpieczeństwa w firmie	Potrafi wskazać, kto w firmie odpowiada za bezpieczeństwo (lub że każdy pracownik ma rolę)	Wywiad swobodny
Uczestnik świadomie odnosi się do roli cyberbezpieczeństwa w środowisku międzynarodowym	Wskazuje nowe wyzwania (np. praca zdalna, chmura, AI)	Wywiad swobodny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

Tak. Zaświadczenia wydawane uczestnikom po odbytym szkoleniu zawierają 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. Zaświadczenie o ukończeniu szkolenia potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane kryteria weryfikacji.

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

Tak. Zaświadczeniu o ukończeniu szkolenia potwierdza, że zarówno proces szkolenia, jak i jego weryfikacja zostały przeprowadzone z uwzględnieniem środków zapewniających niezależność tych etapów.

Program

Moduł 1: Co to jest transformacja cyfrowa i dlaczego trzeba ją zabezpieczyć?

- Czym jest transformacja cyfrowa (na prostych przykładach)
- Jakie zagrożenia niesie cyfryzacja – historia prawdziwych ataków
- Po co firmie cyberbezpieczeństwo (praktyczne skutki ataku: koszty, wizerunek, przestoje)
- Co to znaczy „chronić dane" i dlaczego to ważne dla każdej firmy
- Prosty test wiedzy i dyskusja: „Czy twoja firma jest gotowa?"

Moduł 2: Jak wygląda cyberatak i jak się przed nim bronić?

- Jak wygląda typowy cyberatak – krok po kroku
- Przykłady ataków phishingowych, wirusów, szantażu (ransomware)
- Jakie zabezpieczenia stosować w praktyce: silne hasła, uwierzytelnianie, kopie zapasowe
- Rola pracowników w ochronie firmy – błędy, które kosztują miliony
- Warsztat: rozpoznaj próbę ataku (na podstawie prawdziwych maili)

Moduł 3: Przepisy prawa i obowiązki firm w Polsce i Europie

- Co mówi RODO o danych i bezpieczeństwie
- Nowe przepisy: NIS2, DORA – co musi robić twoja firma?
- Jakie kary grożą za zaniedbania i co sprawdza kontrola?
- Przykłady dokumentów i polityk, które warto mieć (prosty język, bez nadmiaru prawniczego żargonu)
- Ćwiczenie: co zrobić, jeśli dojdzie do wycieku danych

Moduł 4: Jak budować bezpieczną firmę – krok po kroku

- Od czego zacząć: lista 10 podstawowych kroków dla każdej firmy
- Jak przygotować politykę bezpieczeństwa w prostych słowach
- Jak szkolić pracowników, żeby nie klikali „w co nie trzeba"
- Jak przygotować plan działania na wypadek ataku lub awarii
- Miniwarsztat: stwórz własny plan reagowania na incydent

Moduł 5: Bezpieczeństwo firmy w świecie globalnym

- Jakie są nowe trendy: sztuczna inteligencja, praca zdalna, chmura
- Co się dzieje, gdy firma działa międzynarodowo (dane, przepisy, zagrożenia)
- Kto może pomóc: CERT, UODO, ENISA, CSIRT – praktyczne kontakty

- Czego uczą nas największe cyberataki na świecie (case studies)
- Zakończenie: podsumowanie wiedzy, pytania i odpowiedzi

- Szkolenie ma charakter praktyczny i aktywizujący w celu wypracowania najkorzystniejszego podejścia praz rozwiązań dla organizacji.
- Warunki niezbędne do spełnienia, aby realizacja usługi pozwoliła na osiągnięcie głównego celu: Aby osiągnąć główny cel usługi, uczestnicy muszą wziąć udział w całym szkoleniu (100% frekwencji), aktywnie uczestniczyć w szkoleniu.
- Szkolenie skierowane jest do pracowników, którzy niezależnie od zajmowanych stanowisk, w swojej codziennej pracy korzystają z infrastruktury IT, systemów informatycznych lub mają dostęp do danych firmowych. Uczestnicy nie muszą posiadać specjalistycznej wiedzy technicznej, ale powinni rozumieć znaczenie bezpiecznego korzystania z narzędzi cyfrowych w środowisku zawodowym. Wymagany jest minimalny staż pracy wynoszący 1 miesiąc.
- Trener na bieżąco - w trakcie trwania usługi weryfikuje postępy i ocenia efekty uczenia. Po zakończonej usłudze zostaje przeprowadzona walidacja, oparta o założone kryteria weryfikacji efektów uczenia się, realizowana jest z zachowaniem rozdzielności funkcji.
- W ramach realizacji szkolenia uczestnicy otrzymują materiały merytoryczne w formie prezentacji. Materiały wysyłane są na adresy mailowe uczestników szkolenia.
- Usługa realizowana jest w godzinach zegarowych (1 godzina zegarowa = 60 minut).
- Przerwy wliczone są w czas trwania szkolenia.

Harmonogram

Liczba przedmiotów/zajęć: 10

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 10 Moduł 1: Co to jest transformacja cyfrowa i dlaczego trzeba ją zabezpieczyć?	Kamil Kamola	03-07-2025	08:00	12:00	04:00
2 z 10 Przerwa	Kamil Kamola	03-07-2025	12:00	12:15	00:15
3 z 10 Moduł 2: Jak wygląda cyberatak i jak się przed nim bronić?	Kamil Kamola	03-07-2025	12:15	16:00	03:45
4 z 10 Moduł 2: Jak wygląda cyberatak i jak się przed nim bronić? c.d.	Kamil Kamola	04-07-2025	08:00	10:00	02:00
5 z 10 Moduł 3: Przepisy prawa i obowiązki firm w Polsce i Europie	Kamil Kamola	04-07-2025	10:00	12:00	02:00
6 z 10 Przerwa	Kamil Kamola	04-07-2025	12:00	12:15	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
7 z 10 Moduł 3: Przepisy prawa i obowiązki firm w Polsce i Europie c.d.	Kamil Kamola	04-07-2025	12:15	16:00	03:45
8 z 10 Moduł 4: Jak budować bezpieczną firmę – krok po kroku	Kamil Kamola	05-07-2025	08:00	12:00	04:00
9 z 10 Przerwa	Kamil Kamola	05-07-2025	12:00	12:15	00:15
10 z 10 Moduł 5: Bezpieczeństwo firmy w świecie globalnym Jakie są nowe trendy: sztuczna inteligencja, praca zdalna, chmura	Kamil Kamola	05-07-2025	12:15	17:00	04:45

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	6 375,00 PLN
Koszt przypadający na 1 uczestnika netto	6 375,00 PLN
Koszt osobogodziny brutto	255,00 PLN
Koszt osobogodziny netto	255,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Kamil Kamola

Przedsiębiorca posiadający 13-letnie doświadczenie zawodowe w branży IT. W trakcie swojej pracy zawodowej kładzie nacisk na rozwój praktycznych umiejętności w zakresie bezpieczeństwa systemów informatycznych pod kątem zgodności z obecnie obowiązującymi przepisami prawa międzynarodowego oraz krajowego. W swojej codziennej pracy koordynuje działania związane z funkcjonowaniem sektora IT przedsiębiorstw prywatnych jak i podmiotów publicznych, świadczy usługi z zakresu m.in. modelowania procesów biznesowych, audytów oraz analiz przedwdrożeniowych. W przeszłości zdobywał doświadczenie zawodowe na stanowisku programisty aplikacji webowych. Osoba posiadająca bogate doświadczenie zawodowe zbudowane na praktyce, a nie jedynie samej teorii. Posiada średnie wykształcenie. Posiada co najmniej 250 godzin doświadczenia w realizacji szkoleń w podobnej tematyce zrealizowanych w ostatnich pięciu latach (60 miesiącach) wstecz od dnia rozpoczęcia szkolenia.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

W ramach realizacji szkolenia uczestnicy otrzymują materiały merytoryczne w formie prezentacji. Materiały wysyłane są na adresy mailowe uczestników szkolenia.

Warunki uczestnictwa

Szkolenie skierowane jest do pracowników, którzy niezależnie od zajmowanych stanowisk, w swojej codziennej pracy korzystają z infrastruktury IT, systemów informatycznych lub mają dostęp do danych firmowych. Uczestnicy nie muszą posiadać specjalistycznej wiedzy technicznej, ale powinni rozumieć znaczenie bezpiecznego korzystania z narzędzi cyfrowych w środowisku zawodowym.

Wymagany jest minimalny staż pracy wynoszący 1 miesiąc.

Koszt szkolenia nie zawiera kosztów dojazdu, zakwaterowania oraz wyżywienia, a także kosztów środków trwałych.

Informacje dodatkowe

Usługa zwolniona z 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)

Adres

ul. 6 Sierpnia 1
24-100 Puławy
woj. lubelskie

Szkolenie odbędzie się w siedzibie firmy EMOTIVO SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

Kontakt

Kamil Kamola

E-mail bur@k2c.com.pl
Telefon (+48) 533 552 510