Możliwość dofinansowania

Zarządzanie ryzykiem cyberbezpieczeństwa i reagowanie na incydenty w organizacji - szkolenie.

Numer usługi 2026/06/22/179479/3641753

1 997,52 PLN brutto
1 624,00 PLN netto
285,36 PLN brutto/h
232,00 PLN netto/h
261,33 PLN cena rynkowa

K2 GROUP SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

4,6 / 5

86 ocen

Puławy
Usługa szkoleniowa
stacjonarna
Zajęcia grupowe
07:00 h
08.08.2026 do 08.08.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie skierowane do właścicieli przedsiębiorstw, członków kadry zarządzającej oraz osób odpowiedzialnych za podejmowanie decyzji dotyczących bezpieczeństwa organizacji. Uczestnikami mogą być osoby nadzorujące procesy biznesowe, ochronę danych, zarządzanie ryzykiem oraz ciągłość działania przedsiębiorstwa. Szkolenie przeznaczone jest dla osób, które chcą zdobyć wiedzę i umiejętności w zakresie identyfikacji zagrożeń cybernetycznych, oceny ryzyka, reagowania na incydenty bezpieczeństwa oraz budowania odporności organizacji na zagrożenia występujące w środowisku cyfrowym. Dzięki zdobytym kompetencjom uczestnicy będą mogli skuteczniej wspierać bezpieczeństwo informacji i stabilność funkcjonowania przedsiębiorstwa.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	2
Data zakończenia rekrutacji	07-08-2026
Forma prowadzenia usługi	stacjonarna
Podstawa uzyskania wpisu do BUR	Certyfikat ISO 21001: 2018 Organizacje edukacyjne – „Systemy zarządzania dla organizacji edukacyjnych – wymagania ze wskazówkami dotyczącymi użytkowania”

Cel

Cel edukacyjny

Szkolenie przygotowuje uczestników do identyfikowania i oceny ryzyk związanych z cyberbezpieczeństwem oraz do podejmowania działań ograniczających skutki incydentów bezpieczeństwa. Uczestnik po zakończeniu szkolenia potrafi rozpoznawać źródła ryzyka, uczestniczyć w procesie zarządzania incydentami, wspierać działania związane z ciągłością działania organizacji oraz stosować procedury reagowania na naruszenia bezpieczeństwa.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik identyfikuje ryzyka cyberbezpieczeństwa występujące w organizacji	definiuje źródła ryzyka; rozróżnia zagrożenia wewnętrzne i zewnętrzne; określa potencjalne skutki incydentów	Wywiad swobodny
Uczestnik analizuje wpływ zagrożeń cybernetycznych na funkcjonowanie organizacji	definiuje konsekwencje utraty poufności, integralności i dostępności informacji; wskazuje obszary szczególnie narażone na ryzyko	Wywiad swobodny
Uczestnik stosuje podstawowe zasady zarządzania ryzykiem cyberbezpieczeństwa	identyfikuje etapy procesu zarządzania ryzykiem; proponuje działania ograniczające ryzyko; wskazuje metody monitorowania zagrożeń	Wywiad swobodny
Uczestnik identyfikuje incydenty bezpieczeństwa i właściwie na nie reaguje	identyfikuje symptomy incydentu; określa sposób zgłoszenia incydentu; wskazuje działania podejmowane po wykryciu zdarzenia	Wywiad swobodny
Uczestnik stosuje zasady ciągłości działania i odtwarzania po awarii	wyjaśnia znaczenie kopii zapasowych; wskazuje działania minimalizujące skutki awarii; opisuje podstawowe procedury odtworzeniowe	Wywiad swobodny
Uczestnik wspiera budowanie kultury cyberbezpieczeństwa w organizacji	wskazuje działania zwiększające świadomość pracowników; omawia znaczenie procedur bezpieczeństwa; identyfikuje dobre praktyki organizacyjne	Wywiad swobodny

Kwalifikacje

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

Moduł I. Zarządzanie ryzykiem cyberbezpieczeństwa

- podstawowe pojęcia związane z ryzykiem,
- źródła zagrożeń cybernetycznych,
- identyfikacja aktywów informacyjnych,
- analiza i ocena ryzyka.

Moduł II. Ochrona organizacji przed cyberzagrożeniami

- działania zapobiegawcze,
- środki organizacyjne i techniczne,
- monitorowanie zagrożeń,
- budowanie odporności organizacji.

Moduł III. Reagowanie na incydenty bezpieczeństwa

- definicja incydentu,
- wykrywanie incydentów,
- procedury zgłaszania,
- role i odpowiedzialności w procesie reagowania.

Moduł IV. Ciągłość działania i odtwarzanie po awarii

- kopie zapasowe,
- odtwarzanie danych,
- minimalizowanie skutków incydentów,
- podstawy planowania ciągłości działania.

Moduł V. Kultura cyberbezpieczeństwa w organizacji

- świadomość pracowników,
- dobre praktyki bezpieczeństwa,
- komunikacja w sytuacjach kryzysowych,
- przykłady rzeczywistych incydentów.

Moduł VI. Warsztaty praktyczne i podsumowanie

- analiza studiów przypadków,
- ćwiczenia z oceny ryzyka,
- ćwiczenia z reagowania na incydenty,
- podsumowanie i omówienie rezultatów szkolenia.

Walidacja

- 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 do właścicieli przedsiębiorstw, członków kadry zarządzającej oraz osób odpowiedzialnych za podejmowanie decyzji dotyczących bezpieczeństwa organizacji. Uczestnikami mogą być osoby nadzorujące procesy biznesowe, ochronę danych, zarządzanie ryzykiem oraz ciągłość działania przedsiębiorstwa. Szkolenie przeznaczone jest dla osób, które chcą zdobyć wiedzę i umiejętności w zakresie identyfikacji zagrożeń cybernetycznych, oceny ryzyka, reagowania na incydenty bezpieczeństwa oraz budowania odporności organizacji na zagrożenia występujące w środowisku cyfrowym. Dzięki zdobytym kompetencjom uczestnicy będą mogli skuteczniej wspierać bezpieczeństwo informacji i stabilność funkcjonowania przedsiębiorstwa.
- 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 i walidacja wliczone są w czas trwania szkolenia.

Harmonogram

Liczba pozycji harmonogramu: 8

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 8 Moduł I. Zarządzanie ryzykiem cyberbezpieczeństwa	Zajęcia	Kamil Kamola	08-08-2026	08:00	08:40	00:40
2 z 8 Moduł II. Ochrona organizacji przed cyberzagrożeniami	Zajęcia	Kamil Kamola	08-08-2026	08:40	09:30	00:50
3 z 8 Moduł III. Reagowanie na incydenty bezpieczeństwa	Zajęcia	Kamil Kamola	08-08-2026	09:30	10:10	00:40
4 z 8 -	Przerwa	-	08-08-2026	10:10	11:10	01:00
5 z 8 Moduł IV. Ciągłość działania i odtwarzanie po awarii	Zajęcia	Kamil Kamola	08-08-2026	11:10	12:30	01:20

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
6 z 8 Moduł V. Kultura cyberbezpieczeństwa w organizacji	Zajęcia	Kamil Kamola	08-08-2026	12:30	13:30	01:00
7 z 8 Moduł VI. Warsztaty praktyczne i podsumowanie	Zajęcia	Kamil Kamola	08-08-2026	13:30	14:30	01:00
8 z 8 -	Walidacja	-	08-08-2026	14:30	15:00	00:30

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	07:00
w tym suma godzin zajęć	05:30
w tym suma godzin walidacji	00:30
w tym suma przerw	01:00
Suma godzin dydaktycznych bez przerw	08:00

Cennik

Jeżeli korzystasz z dofinansowania i usługa stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego wraz z usługą lub dostawą towarów ściśle związaną z usługami kształcenia zawodowego lub przekwalifikowania zawodowego to możesz mieć możliwość skorzystania za zwolnienia z podatku VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2024 r. o podatku od towarów i usług, jeśli usługa w całości jest finansowana ze środków publicznych lub § 3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień w przypadku, gdy usługa jest finansowana w co najmniej 70% ze środków publicznych.

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 997,52 PLN
Koszt przypadający na 1 uczestnika netto	1 624,00 PLN

Koszt osobogodziny brutto	285,36 PLN
Koszt osobogodziny netto	232,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	07:00

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 do właścicieli przedsiębiorstw, członków kadry zarządzającej oraz osób odpowiedzialnych za podejmowanie decyzji dotyczących bezpieczeństwa organizacji. Uczestnikami mogą być osoby nadzorujące procesy biznesowe, ochronę danych, zarządzanie ryzykiem oraz ciągłość działania przedsiębiorstwa. Szkolenie przeznaczone jest dla osób, które chcą zdobyć wiedzę i umiejętności w zakresie identyfikacji zagrożeń cybernetycznych, oceny ryzyka, reagowania na incydenty bezpieczeństwa oraz budowania odporności organizacji na zagrożenia występujące w środowisku cyfrowym. Dzięki zdobytym kompetencjom uczestnicy będą mogli skuteczniej wspierać bezpieczeństwo informacji i stabilność funkcjonowania przedsiębiorstwa.

Informacje dodatkowe

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

Adres

ul. Dęblińska 18
24-100 Puławy
woj. lubelskie

Szkolenie odbędzie się w siedzibie firmy K2 Group sp. z o.o. w sali konferencyjnej.

Kontakt

ANDŻELIKA IWANICZ

E-mail a.iwanicz@k2g.com.pl
Telefon (+48) 533 552 510