Możliwość dofinansowania

Cyberbezpieczeństwo dla pracowników biurowych i administracyjnych — praktyczne szkolenie z cyberhigieny, ochrony danych i reagowania na incydenty

Numer usługi 2026/06/22/161638/3641257

6 543,60 PLN brutto
5 320,00 PLN netto
186,96 PLN brutto/h
152,00 PLN netto/h
261,33 PLN cena rynkowa

KORYCKI & GRACZYK CONSULTING GROUP SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

4,9 / 5

720 ocen

Usługa szkoleniowa
zdalna w czasie rzeczywistym
Zajęcia grupowe
35:00 h
03.08.2026 do 07.08.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikatory projektów	Kierunek - Rozwój, Nowy start w Małopolsce z EURESEM, Małopolski Pociąg do kariery, Zachodniopomorskie Bony Szkoleniowe
Grupa docelowa usługi	• Pracownicy biurowi, administracja, sekretariaty, recepcje, kancelarie, działy kadr, księgowości, obsługi klienta, back-office itp. • Pracownicy jednostek administracji publicznej oraz firm prywatnych przetwarzający dane i informacje (w tym dane osobowe). • Osoby przygotowujące się do pracy na stanowiskach administracyjnych. • Uczestnicy projektów: **Małopolski Pociąg do Kariery**, **Nowy Start w Małopolsce (EURES)**, **Kierunek Rozwój**. • Usługa rozwojowa adresowana również dla Uczestników projektu **Zachodniopomorskie Bony Szkoleniowe.** **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	2
Maksymalna liczba uczestników	30
Data zakończenia rekrutacji	02-08-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Usługa pn. "Cyberbezpieczeństwo dla pracowników biurowych i administracyjnych — praktyczne szkolenie z cyberhigieny, ochrony danych i reagowania na incydenty" 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.	Rozróżnia pojęcia na podstawie opisanych sytuacji	Test teoretyczny z wynikiem generowanym automatycznie
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 z wynikiem generowanym automatycznie
Definiuje znaczenie aktualizacji oprogramowania w kontekście zabezpieczeń cyfrowych.	Uczestnik wyjaśnia, dlaczego regularne aktualizacje oprogramowania są kluczowe dla zachowania bezpieczeństwa systemów i danych.	Test teoretyczny z wynikiem generowanym automatycznie
Dobiera zasady tworzenia i zarządzania bezpiecznymi hasłami do opisanych sytuacji zawodowych	Uczestnik wskazuje cechy silnego hasła frazowego i rozpoznaje błędy w schematach haseł, korzysta z menedżerów haseł do ich przechowywania.	Test teoretyczny z wynikiem generowanym automatycznie
Identyfikuje i reaguje na próby phishingu i inne oszustwa internetowe.	Uczestnik poprawnie identyfikuje fałszywe wiadomości e-mail i strony internetowe oraz wskazuje właściwą kolejność działań w procedurze reagowania na incydent.	Test teoretyczny z wynikiem generowanym automatycznie
Stosuje zasady bezpiecznego korzystania z sieci publicznych i prywatnych.	Uczestnik rozpoznaje zasady bezpiecznego korzystania z sieci publicznych i prywatnych i stosuje praktyki ochrony prywatności.	Test teoretyczny z wynikiem generowanym automatycznie

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

DZIEŃ 1

08:00 – 09:00: Wprowadzenie do szkolenia - wideokonferencja — TEORIA

Kwestie organizacyjne, omówienie celów 5-dniowego programu, kontrakt grupowy oraz zasady zachowania poufności danych organizacji uczestników.

09:00 – 10:00: Samoocena bezpieczeństwa stanowiska pracy - miniaudyt użytkownika - ćwiczenia — PRAKTYKA (1h)

Warsztat z samodzielnej identyfikacji zasobów cyfrowych na stanowisku pracy. Tworzenie uproszczonej mapy ryzyk i podatności stanowiskowych.

10:00 – 10:30: Przerwa (30 min)

10:30 – 11:30: Istota i podstawowe terminy w zakresie cyberbezpieczeństwa - wideokonferencja — TEORIA (1h)

Wyjaśnienie triady poufności, integralności i dostępności (CIA). Omówienie roli pracownika w systemie obrony i skutków finansowo-prawnych wycieków.

11:30 – 12:30 Podstawy prawne cyberbezpieczeństwa i zalecenia ENISA - wideokonferencja — TEORIA (1h)

Przegląd polskich i unijnych regulacji prawnych. Omówienie kluczowych wytycznych Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) dla biur.

12:30 – 13:00 Przerwa (30 min)

13:00 – 15:00 Najpopularniejsze ataki cybernetyczne - ćwiczenia — PRAKTYKA (2h)

Analiza studiów przypadku (*case studies*) dotyczących złośliwego oprogramowania i ransomware. Warsztat z rozpoznawania infekcji komputera.

DZIEŃ 2

08:00 – 09:00 Phishing - ćwiczenia — PRAKTYKA (1h)

Praktyczna detekcja fałszywych wiadomości e-mail i SMS (smishing). Analiza nagłówków, podejrzanych linków oraz technik manipulacji.

09:00 – 10:00 Przestępstwa finansowe w przestrzeni cyfrowej - ćwiczenia — PRAKTYKA (1h)

Rozpracowanie oszustw typu BEC (fałszywe faktury, podmiana kont) oraz mechanizmu wyłudzeń „na prezesa”. Praca na scenariuszach zagrożeń.

10:00 – 10:30 Przerwa (30 min)

10:30 – 11:30 Zasady ustalania haseł zgodnie z obecnymi standardami bezpieczeństwa cyfrowego - wideokonferencja — TEORIA (1h)

Omówienie nowoczesnych standardów (NIST, KRI). Obalenie mitów o częstej zmianie haseł, zasady konstruowania silnych haseł frazowych.

11:30 – 12:30 Jak działa i jak wybrać menadżera haseł? - wideokonferencja — TEORIA (1h)

Architektura baz haseł, znaczenie hasła głównego (*Master Password*). Porównanie i kryteria wyboru menadżera haseł do użytku służbowego.

12:30 – 13:00 Przerwa (30 min)

13:00 – 15:00 Dlaczego tak często hakerzy łamią hasła? - wideokonferencja z ćwiczeniami — TEORIA (1h) + PRAKTYKA (1h)

- **Zakres (Teoria 13:00-14:00):** Mechanika ataków słownikowych, brute-force oraz zjawisko wtórnego użycia haseł (*credential stuffing*).
- **Zakres (Praktyka 14:00-15:00):** Analiza zanonimizowanych i syntetycznych przykładów haseł inspirowanych publicznymi raportami o wyciekach, bez wykorzystywania rzeczywistych danych osobowych lub poświadczeń.

DZIEŃ 3

08:00 – 09:00 Dlaczego samo hasło nie wystarczy? Autoryzacja dwuskładnikowa w praktyce - wideokonferencja — TEORIA (1h)

Słabości zabezpieczeń jednoskładnikowych. Wprowadzenie do MFA/2FA: omówienie działania aplikacji autoryzujących, kodów i kluczy U2F.

09:00 – 10:00 Szyfrowanie plików, folderów i pendrive'ów w praktyce - ćwiczenia — PRAKTYKA (1h)

Warsztat z obsługi programów szyfrujących (BitLocker, 7-Zip). Procedura bezpiecznej wysyłki załączników i przekazywania haseł innym kanałem.

10:00 – 10:30 Przerwa (30 min)

10:30 – 11:30 Jak chronić dane osobowe zgodnie z RODO? - wideokonferencja — TEORIA (1h)

Zasady przetwarzania danych w pracy administracyjnej. Identyfikacja ryzyka incydentów i procedury raportowania do Inspektora Ochrony Danych.

11:30 – 12:30 Zastrzeż swój PESEL - ćwiczenia — PRAKTYKA (1h)

Instruktaż krok po kroku konfiguracji usługi w systemie mObywatel/Obywatel.gov.pl. Analiza skutków prawnych ochrony przed wyłudzeniami. Ochrona tożsamości cyfrowej pracownika i przeciwdziałanie wyłudzeniom danych identyfikacyjnych.

12:30 – 13:00 Przerwa (30 min)

13:00 – 15:00 Jak robić backup danych? - ćwiczenia — PRAKTYKA (2h)

Wdrożenie reguły 3-2-1 w codziennych obowiązkach. Samodzielne tworzenie kopii zapasowych plików i poczty na dyskach sieciowych według procedury.

DZIEŃ 4

08:00 – 09:00 Dlaczego warto korzystać z „chmury"? - wideokonferencja — TEORIA (1h)

Bezpieczeństwo danych w chmurze (OneDrive, SharePoint) vs serwer lokalny. Zasada współdzielonej odpowiedzialności i kontroli uprawnień.

09:00 – 10:00 Wykorzystywanie AI przez cyberprzestępców – jak nie dać się nabrać? wideokonferencja — TEORIA (1h)

Wykorzystanie sztucznej inteligencji do generowania spersonalizowanego phishingu i automatyzacji cyberataków. Nowe wektory zagrożeń.

10:00 – 10:30 Przerwa (30 min)

10:30 – 11:30 Jak zabezpieczyć swój sprzęt i prywatność? Programy antywirusowe, firewall, tryb incognito, cookies, VPN - ćwiczenia — PRAKTYKA (1h)

Konfiguracja podstawowych barier ochronnych na komputerze. Zarządzanie prywatnością w przeglądarce i bezpieczne korzystanie z sieci przez VPN.

11:30 – 12:30 Co o nas wiedzą? - socjotechniki wykorzystywane przez hakerów - wideokonferencja — TEORIA (1h)

Psychologia manipulacji (reguła autorytetu, lęku, pilności). Zagrożenia płynące z białego wywiadu (OSINT) i upubliczniania danych w social mediach.

12:30 – 13:00 Przerwa (30 min)

13:00 – 15:00 Co zrobić, gdy zostanę zaatakowany? Procedura formalna i komunikacyjna - ćwiczenia — PRAKTYKA (2h)

Trening reagowania na incydent według ścieżki: izolacja sprzętu -> powiadomienie IT -> raport formalny. Praca na schematach blokowych.

DZIEŃ 5

08:00 – 09:00 Jak wzmocnić kulturę cyberbezpieczeństwa w organizacji? - wideokonferencja — TEORIA (1h)

Budowanie nawyków zespołowych: blokowanie stacji roboczej (Win+L), zasada czystego biurka/ekranu, bezpieczna utylizacja dokumentów.

09:00 – 10:00 Jak rodzą się fake newsy przez wykorzystywanie narzędzi AI? - wideokonferencja — TEORIA (1h)

Mechanizmy dezinformacji. Identyfikacja i zagrożenia związane z materiałami typu Deepfake (fałszowanie głosu przełożonego, wizerunku firmy).

10:00 – 10:30 Przerwa (30 min)

10:30 – 11:30 Ćwiczenie grupowe: symulacje ataków cybernetycznych - ćwiczenia — PRAKTYKA (1h)

Gra symulacyjna (table-top). Podejmowanie decyzji pod presją czasu w sytuacji wielopoziomowego kryzysu naruszenia bezpieczeństwa w biurze.

11:30 – 12:30 Narzędzia i programy wzmacniające bezpieczeństwo cyfrowe - ćwiczenia — PRAKTYKA (1h)

Dobór i instalacja przydatnych rozszerzeń przeglądarek (blokery skryptów) oraz weryfikacja wycieków poświadczeń w serwisach zewnętrznych.

12:30 – 13:00 Przerwa (30 min)

13:00 – 14:00 Podsumowanie — TEORIA (1h)

Sesja Q&A, usystematyzowanie wiedzy z 5 dni szkolenia, ewaluacja i sformułowanie osobistych wniosków wdrożeniowych na stanowisku pracy.

14:00 – 15:00 Test teoretyczny z wynikiem generowanym automatycznie — WALIDACJA (1h)

Walidacja efektów uczenia się zostanie przeprowadzona w formie testu online w Google Forms, udostępnionego uczestnikom podczas spotkania realizowanego na platformie Google Meet.

1) Godziny i forma

Szkolenie trwa łącznie **35 godzin zegarowych** (1 godzina = 60 minut). Przerwy wliczane są w czas trwania usługi. Usługa realizowana jest zdalnie w czasie rzeczywistym, na platformie Google Meet. Szkolenie przewidziane jest od dwóch do trzydziestu osób.

Bilans struktury czasu usługi (5 dni):

- **Część teoretyczna i organizacyjno-teoretyczna:** 14 godzin 00 minut (840 minut)
- **Część praktyczna (warsztaty, ćwiczenia, symulacje):** 15 godzin 00 minut (900 minut)
- **Walidacja (test wiedzy online):** 1 godzina 00 minut (60 minut)
- **Przerwy (ujęte w harmonogramie):** 5 godzin 00 minut (300 minut)
  - **Łączny czas trwania usługi:** 35 godzin zegarowych (2100 minut)

2) Metoda prowadzenia

Zajęcia prowadzone są metodami interaktywnymi i aktywizującymi, umożliwiającymi uczenie się w oparciu o doświadczenie: krótkie wprowadzenia trenera, studia przypadków (*case studies*), ćwiczenia indywidualne i grupowe, quizy on-line, dyskusje moderowane, odgrywanie scenek sytuacyjnych, praca na checklistach i prostych procedurach biurowych.

3) Grupa docelowa

- Pracownicy biurowi, administracja, sekretariaty, recepcje, kancelarie, działy kadr, księgowości, obsługi klienta, back-office itp.
- Pracownicy jednostek administracji publicznej oraz firm prywatnych przetwarzający dane i informacje (w tym dane osobowe).
- Osoby przygotowujące się do pracy na stanowiskach administracyjnych.

- Uczestnicy projektów: **Małopolski Pociąg do Kariery**, **Nowy Start w Małopolsce (EURES)**, **Kierunek Rozwój**.
- Usługa rozwojowa adresowana również dla Uczestników projektu **Zachodniopomorskie Bony Szkoleniowe.**

Szkolenie jest przeznaczone przede wszystkim dla osób chcących chronić dane firmy, rozpoznawać oszustwa np. w mediach społecznościowych oraz odpowiednio reagować na nie.

4) Cel edukacyjny

Usługa pn. "Cyberbezpieczeństwo dla pracowników biurowych i administracyjnych — praktyczne szkolenie z cyberhigieny, ochrony danych i reagowania na incydenty" 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.

5) Walidacja

Walidacja realizowana jest poprzez test online z wynikiem generowanym automatycznie w Google Forms. Test obejmuje pytania zamknięte jednokrotnego wyboru odnoszące się do efektów uczenia się i kryteriów ich weryfikacji określonych w Karcie Usługi. Test zawiera pytania sytuacyjne i scenariuszowe, w których uczestnik dobiera właściwe działania, kolejność reakcji oraz narzędzia bezpieczeństwa do opisanych przypadków zawodowych. Wynik testu generowany jest automatycznie przez system po zakończeniu testu, bez udziału osoby prowadzącej szkolenie w ocenie odpowiedzi. Warunkiem uzyskania pozytywnego wyniku walidacji jest uzyskanie minimum 80% poprawnych odpowiedzi. Osoba prowadząca szkolenie nie dokonuje oceny odpowiedzi, nie ingeruje w wynik testu i nie podejmuje decyzji walidacyjnej. Wynik generowany jest automatycznie przez system na podstawie klucza odpowiedzi. Uczestnik przystępuje do testu samodzielnie, zgodnie z instrukcją przekazaną przed rozpoczęciem walidacji.

Harmonogram

Liczba pozycji harmonogramu: 36

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 36 Wprowadzenie do szkolenia - wideokonferencja	Zajęcia	DOMINIK HAMERA	03-08-2026	08:00	09:00	01:00
2 z 36 Samoocena bezpieczeństwa stanowiska pracy - miniaudyt użytkownika - ćwiczenia	Zajęcia	DOMINIK HAMERA	03-08-2026	09:00	10:00	01:00
3 z 36 -	Przerwa	-	03-08-2026	10:00	10:30	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
4 z 36 Istota i podstawowe terminy w zakresie cyberbezpieczeństwa - wideokonferencja	Zajęcia	DOMINIK HAMERA	03-08-2026	10:30	11:30	01:00
5 z 36 Podstawy prawne cyberbezpieczeństwa i zalecenia ENISA - wideokonferencja	Zajęcia	DOMINIK HAMERA	03-08-2026	11:30	12:30	01:00
6 z 36 -	Przerwa	-	03-08-2026	12:30	13:00	00:30
7 z 36 Najpopularniejsze ataki cybernetyczne - ćwiczenia	Zajęcia	DOMINIK HAMERA	03-08-2026	13:00	15:00	02:00
8 z 36 Phishing - ćwiczenia	Zajęcia	DOMINIK HAMERA	04-08-2026	08:00	09:00	01:00
9 z 36 Przestępstwa finansowe w przestrzeni cyfrowej - ćwiczenia	Zajęcia	DOMINIK HAMERA	04-08-2026	09:00	10:00	01:00
10 z 36 -	Przerwa	-	04-08-2026	10:00	10:30	00:30
11 z 36 Zasady ustalania haseł zgodnie z obecnymi standardami bezpieczeństwa cyfrowego - wideokonferencja	Zajęcia	DOMINIK HAMERA	04-08-2026	10:30	11:30	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
12 z 36 Jak działa i jak wybrać menadżera haseł? - wideokonferencja	Zajęcia	DOMINIK HAMERA	04-08-2026	11:30	12:30	01:00
13 z 36 -	Przerwa	-	04-08-2026	12:30	13:00	00:30
14 z 36 Dlaczego tak często hakerzy łamią hasła? - wideokonferencja z ćwiczeniami	Zajęcia	DOMINIK HAMERA	04-08-2026	13:00	15:00	02:00
15 z 36 Dlaczego samo hasło nie wystarczy? Autoryzacja dwuskładnikowa w praktyce - wideokonferencja	Zajęcia	DOMINIK HAMERA	05-08-2026	08:00	09:00	01:00
16 z 36 Szyfrowanie plików,folderów i pendrive'ów w praktyce - ćwiczenia	Zajęcia	DOMINIK HAMERA	05-08-2026	09:00	10:00	01:00
17 z 36 -	Przerwa	-	05-08-2026	10:00	10:30	00:30
18 z 36 Jak chronić dane osobowe zgodnie z RODO? - wideokonferencja	Zajęcia	DOMINIK HAMERA	05-08-2026	10:30	11:30	01:00
19 z 36 Zastrzeż swój PESEL - ćwiczenia	Zajęcia	DOMINIK HAMERA	05-08-2026	11:30	12:30	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
20 z 36 -	Przerwa	-	05-08-2026	12:30	13:00	00:30
21 z 36 Jak robić backup danych? - ćwiczenia	Zajęcia	DOMINIK HAMERA	05-08-2026	13:00	15:00	02:00
22 z 36 Dlaczego warto korzystać z „chmury”? - wideokonferencja	Zajęcia	DOMINIK HAMERA	06-08-2026	08:00	09:00	01:00
23 z 36 Wykorzystywanie AI przez cyberprzestępców – jak nie dać się nabrać? - wideokonferencja	Zajęcia	DOMINIK HAMERA	06-08-2026	09:00	10:00	01:00
24 z 36 -	Przerwa	-	06-08-2026	10:00	10:30	00:30
25 z 36 Jak zabezpieczyć swój sprzęt i prywatność? Programy antywirusowe, firewall, tryb incognito, cookies, VPN - ćwiczenia	Zajęcia	DOMINIK HAMERA	06-08-2026	10:30	11:30	01:00
26 z 36 Co o nas wiedzą? - socjotechniki wykorzystywane przez hakerów - wideokonferencja	Zajęcia	DOMINIK HAMERA	06-08-2026	11:30	12:30	01:00
27 z 36 -	Przerwa	-	06-08-2026	12:30	13:00	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
28 z 36 Co zrobić, gdy zostanę zaatakowany? Procedura formalna i komunikacyjna - ćwiczenia	Zajęcia	DOMINIK HAMERA	06-08-2026	13:00	15:00	02:00
29 z 36 Jak wzmocnić kulturę cyberbezpieczeństwa w organizacji? - wideokonferencja	Zajęcia	DOMINIK HAMERA	07-08-2026	08:00	09:00	01:00
30 z 36 Jak rodzą się fake newsy przez wykorzystywanie narzędzi AI? - wideokonferencja	Zajęcia	DOMINIK HAMERA	07-08-2026	09:00	10:00	01:00
31 z 36 -	Przerwa	-	07-08-2026	10:00	10:30	00:30
32 z 36 Ćwiczenie grupowe: symulacje ataków cybernetycznych - ćwiczenia	Zajęcia	DOMINIK HAMERA	07-08-2026	10:30	11:30	01:00
33 z 36 Narzędzia i programy wzmacniające bezpieczeństwo cyfrowe - ćwiczenia	Zajęcia	DOMINIK HAMERA	07-08-2026	11:30	12:30	01:00
34 z 36 -	Przerwa	-	07-08-2026	12:30	13:00	00:30
35 z 36 Podsumowanie	Zajęcia	DOMINIK HAMERA	07-08-2026	13:00	14:00	01:00
36 z 36 -	Walidacja	DOMINIK HAMERA	07-08-2026	14:00	15:00	01:00

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	35:00
w tym suma godzin zajęć	29:00
w tym suma godzin walidacji	01:00
w tym suma przerw	05:00
Suma godzin dydaktycznych bez przerw	40:00

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	6 543,60 PLN
Koszt przypadający na 1 uczestnika netto	5 320,00 PLN
Koszt osobogodziny brutto	186,96 PLN
Koszt osobogodziny netto	152,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	35:00

Prowadzący

Liczba prowadzących: 1

1 z 1

DOMINIK HAMERA

Doświadczony doradca biznesowy i szkoleniowiec z 10-letnim stażem, specjalizujący się w optymalizacji procesów organizacyjnych, zarządzaniu ryzykiem oraz wdrażaniu procedur zapewniających ciągłość działania firm. Absolwent AWF Warszawa (specjalność: Menedżer). W ramach dotychczasowej praktyki skutecznie pozyskał ponad 200 mln zł dla klientów, co wiązało się z projektowaniem i audytowaniem restrykcyjnych procedur ochrony informacji, poufności oraz bezpieczeństwa danych finansowych i osobowych zgodnie ze standardami unijnymi.

Jako trener z dorobkiem ponad 2000 godzin szkoleniowych i 3000 przeszkolonych osób, specjalizuje się w podnoszeniu kompetencji kadry menedżerskiej z zakresu bezpieczeństwa organizacyjnego, ochrony zasobów przedsiębiorstwa oraz przeciwdziałania zagrożeniom wynikającym z tzw. czynnika ludzkiego (w tym budowanie odporności organizacji na stres i sytuacje kryzysowe). Łączy twarde podejście procesowe z psychologią zarządzania, pomagając sektorowi MŚP i kadrze zarządzającej wdrażać bezpieczne i efektywne modele biznesowe.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały zostaną przekazane drogą elektroniczną. Uczestnik otrzyma skrypty w formacie PDF oraz materiały wideo/linki do materiałów wideo.

Warunki uczestnictwa

- Podstawowa obsługa komputera i poczty elektronicznej.
- Ukończony 18 rok życia

Informacje dodatkowe

1. W przypadku, gdy szkolenie dofinansowane jest w co najmniej 70% ze środków publicznych, usługa korzysta ze zwolnienia z podatku VAT na podstawie § 3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług (t.j. Dz.U. z 2025 r. poz. 832).
2. Uczestnik szkolenia otrzyma zaświadczenie o ukończeniu szkolenia dopiero po pozytywnym wyniku walidacji. Warunkiem otrzymania zaświadczenia o ukończeniu szkolenia jest **pozytywny wynik walidacji** oraz **frekwencja na minimalnym poziomie 80%**.

Warunki techniczne

1. **Platforma komunikacyjna** – Google Meet.

2. **Wymagania sprzętowe:**

- komputer z aktualnym systemem (Windows 10 lub nowszy / macOS 12 lub nowszy / aktualna dystrybucja Linux),
- aktualna przeglądarka (Chrome/Edge/Firefox/Safari – co najmniej dwie ostatnie wersje),
- stabilne łącze internetowe o przepustowości min. 10 Mb/s (pobieranie) i 2 Mb/s (wysyłanie),
- sprawna kamera komputerowa i mikrofon,
- sprawne słuchawki/ głośniki.

Wszystkie działania konfiguracyjne i instalacyjne wykonywane są z uwzględnieniem polityki bezpieczeństwa organizacji uczestnika. **W przypadku sprzętu służbowego uczestnik nie instaluje narzędzi bez zgody administratora IT.**

Okres ważności linku: od godziny zegarowej przed godziną rozpoczęcia szkolenia w dniu pierwszym do godziny zegarowej po zakończeniu szkolenia w dniu ostatnim.

Kontakt

NATALIA DYMEK

E-mail nataliadymek.praca@gmail.com
Telefon (+48) 661 336 570