Możliwość dofinansowania

Cyberbezpieczeństwo i ochrona danych osobistych w przedsiębiorstwie - usługa zdalna na platformie e-LEA

Numer usługi 2026/01/29/150363/3292381

3 444,00 PLN brutto
2 800,00 PLN netto
215,25 PLN brutto/h
175,00 PLN netto/h

PRZEDSIĘBIORSTWO KONSULTINGOWE AGM SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

4,8 / 5

236 ocen

Usługa szkoleniowa
zdalna
16:00 h
10.11.2026 do 11.11.2026

Informacje podstawowe

Kategoria	Biznes / Zarządzanie zasobami ludzkimi
Grupa docelowa usługi	Usługa jest skierowana do przedsiębiorców, pracowników firm, studentów oraz osób bezrobotnych, dostosowując ofertę do ich indywidualnych potrzeb i oczekiwań.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	5
Data zakończenia rekrutacji	09-11-2026
Forma prowadzenia usługi	zdalna
Liczba godzin usługi	16
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

Kurs przygotowuje uczestnika do rozpoznawania i zapobiegania zagrożeniom cyfrowym, reagowania na incydenty bezpieczeństwa oraz wdrażania w organizacji skutecznych praktyk w zakresie ochrony danych osobowych i informacji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
1. Uczestnik zna podstawowe pojęcia i zasady z zakresu cyberbezpieczeństwa oraz ochrony danych osobowych.	Potrafi wskazać rodzaje zagrożeń cyfrowych i naruszeń danych osobowych; rozumie znaczenie bezpieczeństwa informacji w przedsiębiorstwie.	Test teoretyczny
2. Zna najczęstsze rodzaje ataków i zagrożeń w środowisku cyfrowym oraz sposoby ich rozpoznawania.	Poprawnie klasyfikuje typy ataków (np. phishing, ransomware, malware) i zna ich skutki dla organizacji.	Test teoretyczny
3. Zna obowiązki wynikające z przepisów RODO oraz zasady przetwarzania danych osobowych w organizacji.	Wymienia podstawowe obowiązki administratora i użytkownika danych oraz zna procedury reagowania na incydenty.	Test teoretyczny
4. Potrafi zastosować w praktyce zasady bezpiecznego korzystania z systemów informatycznych i zasobów sieciowych.	Stosuje zasady tworzenia bezpiecznych haseł, uwierzytelniania i zarządzania dostępami; potrafi rozpoznać niebezpieczne zachowania użytkowników.	Obserwacja w warunkach rzeczywistych
5. Umie reagować na incydenty bezpieczeństwa oraz wdrażać podstawowe procedury ograniczające skutki naruszeń.	Poprawnie opisuje etapy postępowania po wykryciu incydentu i potrafi wskazać właściwe działania zapobiegawcze.	Obserwacja w warunkach rzeczywistych
6. Potrafi wykorzystać wiedzę o cyberzagrożeniach do opracowania zasad bezpieczeństwa dla swojego stanowiska pracy.	Opracowuje prosty zestaw dobrych praktyk lub checklistę zabezpieczeń.	Obserwacja w warunkach rzeczywistych
7. Rozumie znaczenie bezpieczeństwa cyfrowego i ochrony danych osobowych jako elementu kultury organizacyjnej.	Wykazuje postawę odpowiedzialności za bezpieczeństwo danych w pracy zespołowej.	Obserwacja w warunkach rzeczywistych
8. Przestrzega zasad etyki cyfrowej, poufności i odpowiedzialnego korzystania z informacji.	Deklaruje przestrzeganie zasad bezpieczeństwa i potrafi wskazać konsekwencje ich łamania.	Obserwacja w warunkach rzeczywistych

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 – Podstawy cyberbezpieczeństwa i zagrożenia w środowisku cyfrowym

Część teoretyczna: 08:00-13:00

- Wprowadzenie do cyberbezpieczeństwa – znaczenie i podstawowe pojęcia.
- Przegląd aktualnych zagrożeń cyfrowych (phishing, malware, ransomware, socjotechnika).

Przerwa 10:00-10:15

- Mechanizmy ochrony przed atakami zabezpieczenia techniczne i organizacyjne.
- Rola pracowników w zapewnianiu bezpieczeństwa informacji.

Przerwa obiadowa 13:00-13:30

Część praktyczna (na platformie e-LEA): 13:30-16:00

- Studium przypadku: analiza przykładowych incydentów bezpieczeństwa.
- Interaktywne quizy i testy wiedzy.
- Tworzenie listy dobrych praktyk bezpieczeństwa dla użytkownika systemu IT.

Dzień 2 – Ochrona danych osobowych i reagowanie na incydenty

Część teoretyczna: 8:00-13:00

- Obowiązki pracowników i administratorów danych zgodnie z RODO.
- Procedury przetwarzania, przechowywania i zabezpieczania danych osobowych.

Przerwa 10:00-10:15

- Postępowanie w przypadku naruszenia bezpieczeństwa danych.
- Odpowiedzialność prawna i etyczna w zakresie ochrony informacji.

Przerwa Obiadowa 13:00-13:30

Część praktyczna (na platformie e-LEA): 13:30-16:00

- Ćwiczenia z identyfikacji naruszeń danych osobowych.
- Tworzenie procedur reagowania na incydenty.
- Test końcowy – weryfikacja wiedzy i umiejętności

Usługa jest realizowana przy wykorzystaniu licencji: Licencja SaaS na okres 24 m-cy, Profesjonalnej Platformy Edukacyjnej e - LEA Enterprise "

dofinansowanej w ramach projektu

Nowa Perspektywa dla BUR" nr FERS.01.01-IP.09-0019/23

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 444,00 PLN
Koszt przypadający na 1 uczestnika netto	2 800,00 PLN
Koszt osobogodziny brutto	215,25 PLN
Koszt osobogodziny netto	175,00 PLN

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymują dostęp do pełnego zestawu materiałów na platformie e-LEA, w tym:

Wideo i wykłady:

- Czym są mikropoświadczenia,
- Wpływ mikropoświadczeń na rynek pracy,
- Standard Open Badge – międzynarodowy system uznawalności,
- Główne elementy skutecznego kursu,
- Tworzenie treści pod kątem mikropoświadczeń,
- Angażowanie uczestników i optymalizacja treści,
- Jak efektywnie wdrażać mikropoświadczenia,
- Konfiguracja mikropoświadczeń na e-LEA.

Ćwiczenia i notatki: materiały tekstowe, instrukcje i podsumowania do każdego modułu.

Egzamin końcowy: test wiedzy online „Mikropoświadczenia i ich wdrażanie” (15 pytań).

Certyfikat i Open Badge: cyfrowe potwierdzenie ukończenia kursu

Warunki techniczne

1. Do korzystania z Usługi Profesjonalnej Platformy Edukacyjnej e-LEA konieczne jest spełnienie następujących warunków technicznych przez komputer lub inne urządzenie Klienta lub Użytkownika Końcowego. Klient zawrze identyczne lub bardziej restrykcyjne wymagania techniczne dla Użytkownika Końcowego Platformy Klienckiej.

- System operacyjny: Windows 7 lub nowszy, MacOS 10.12 lub nowszy.
- Pamięć operacyjna: co najmniej 4 GB, optymalnie 8 GB i więcej; w przypadku komputerów z systemem Windows 8 lub nowszym zaleca się minimum 8 GB RAM.
- Urządzenia peryferyjne lub wbudowane: słuchawki i mikrofon (lub głośniki i mikrofon), kamera internetowa – wymagane do udziału w wykładach LIVE.
- Ekran: rozdzielczość co najmniej 1280×768.
- Miejsce na dysku: 20 MB wolnego miejsca.
- Internet: stabilne łącze o parametrach:
- pobieranie powyżej 512 kbps (jakość SD),

- pobieranie powyżej 2 Mbps (jakość HD),
- pobieranie i wysyłanie powyżej 10 Mbps (jakość Full HD, udział w wydarzeniach online),
- opóźnienie do 40 ms.
- Rekomendowane parametry internetu: pobieranie i wysyłanie od 30 Mbps, opóźnienie do 40 ms.
- Przeglądarka: aktualna wersja Chrome, Safari, Firefox lub Edge z obsługą plików audio i wideo.
- Adres e-mail: aktywny adres e-mail uczestnika.
- Urządzenia mobilne: aplikacja e-LEA pobrana z Google Play (Android) lub App Store (iOS).
- Karta graficzna: opcjonalna, zwiększa płynność i wydajność przy dużej liczbie grafik i filmów.
- Karta dźwiękowa: opcjonalna; w przypadku jej braku dźwięk odtwarzany jest przez urządzenia peryferyjne lub wbudowane.

1. Usługa Profesjonalnej Platformy Edukacyjnej e-LEA jest świadczona w modelu SaaS (Software as a Service), co oznacza, że oprogramowanie platformy jest instalowane i utrzymywane w całości w ramach infrastruktury e-LEA oraz udostępniane Klientowi online.
2. Klient w trakcie, przed i po okresie użytkowania nie nabywa jakichkolwiek praw do oprogramowania Platformy.

Kontakt

Jagoda Borek

E-mail jborek@agm-konsulting.pl

Telefon (+48) 539 069 128