Możliwość dofinansowania

„Cyberbezpieczeństwo w organizacji: jak rozpoznać i eliminować zagrożenia” - usługa zdalna na platformie e-Lea

Numer usługi 2026/01/16/194418/3262971

430,50 PLN brutto
350,00 PLN netto
143,50 PLN brutto/h
116,67 PLN netto/h

FU2RES SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

Brak ocen dla tego dostawcy

zdalna
Usługa szkoleniowa
3 h
21.01.2026 do 30.01.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Pracownicy biurowi, kadra menedżerska i administracyjna, Firmy i instytucje z całej Polski (MŚP i duże podmioty), Uczestnicy indywidualni zainteresowani podnoszeniem świadomości w zakresie bezpieczeństwa cyfrowego. Potrzeby: redukcja ryzyka incydentów, poprawa higieny pracy cyfrowej, znajomość procedur reagowania, elastyczny dostęp online.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	100
Data zakończenia rekrutacji	29-01-2026
Forma prowadzenia usługi	zdalna
Liczba godzin usługi	3
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

Profilaktyka i prewencja – silny nacisk na zapobieganie incydentom (cyberhigiena codzienna, checklisty dobrych praktyk), a nie tylko na reagowanie po
fakcie.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Najczęstsze zagrożenia w pracy biurowej	Uczestnik zna definicje "Spoofingu"	Test teoretyczny z wynikiem generowanym automatycznie
Zarządzanie hasłami i tożsamością	Uczestnik jest w stanie rozpoznać definicje "Menedżera haseł"	Test teoretyczny z wynikiem generowanym automatycznie
Bezpieczeństwo poczty elektronicznej i komunikacji	Uczestnik jest w stanie rozpoznać niebezpieczne sytuacje: np. czy "załącznik docx. od nieznanego dostawcy"	Test teoretyczny z wynikiem generowanym automatycznie
Bezpieczna praca biurowa i zdalna	Uczestnik jest w stanie określić czego należy unikac podczas pracy w "chmurze"	Test teoretyczny z wynikiem generowanym automatycznie
Ochrona danych osobowych i firmowych	Uczestnik jest w stanie określić czym jest "polityka" czystego biurka"	Test teoretyczny z wynikiem generowanym automatycznie
Reagowanie na incydenty	Uczestnik wie jak zareagować, kiedy jego komputer zostanie zablokowany /przejęty przez osoby do tego nie powołane	Test teoretyczny z wynikiem generowanym automatycznie
Dobre praktyki i podsumowanie szkolenia cyberbezpieczeństwo w biurze	Uczestnik jest w stanie określić czynności tzw. "Cyberhigieny"	Test teoretyczny z wynikiem generowanym automatycznie

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

Usługa jest realizowana przy wykorzystaniu licencji "SaaS e-LEA Enterprise" dofinansowanej w ramach projektu „Nowa perspektywa dla BUR” nr FERS.01.03-IP.09-0019/23

1. Wprowadzenie do cyberbezpieczeństwa

- Dlaczego cyberbezpieczeństwo dotyczy każdego pracownika biurowego.
- Przykłady realnych incydentów w firmach i ich skutki.
- Związek między bezpieczeństwem prywatnym a zawodowym.

2. Najczęstsze zagrożenia w pracy biurowej

- Phishing – fałszywe maile i komunikaty.
- Smishing i vishing – oszustwa telefoniczne i SMS.
- Ransomware – blokowanie danych i szantaż.
- Malware i fałszywe aktualizacje.
- Spoofing i fałszywe strony logowania.

3. Zarządzanie hasłami i tożsamością

- Jak tworzyć i zapamiętywać silne hasła.
- Rola menedżerów haseł.
- Wieloskładnikowe uwierzytelnianie (MFA).
- Najczęstsze błędy pracowników związane z hasłami.

4. Bezpieczeństwo poczty elektronicznej i komunikacji

- Jak rozpoznać podejrzane wiadomości i załączniki.
- Zasady bezpiecznej komunikacji służbowej i prywatnej.
- Ochrona danych przesyłanych mailem i w komunikatorach.

5. Bezpieczna praca biurowa i zdalna

- Podstawowe zasady ochrony komputera i smartfona.
- Aktualizacje i legalne oprogramowanie.
- Praca w chmurze – co robić, a czego unikać.
- Bezpieczne korzystanie z publicznych sieci Wi-Fi.

6. Ochrona danych osobowych i firmowych

- Podstawowe zasady zgodne z RODO.
- Jak nie dopuścić do wycieku danych z biura.
- Przechowywanie i niszczenie dokumentów (papierowych i cyfrowych).

7. Człowiek jako najsłabsze i najmocniejsze ogniwo

- Socjotechnika – jak cyberprzestępcy manipulują ludźmi.
- Budowanie świadomości i kultury bezpieczeństwa w pracy.
- Dlaczego warto zgłaszać incydenty.

8. Reagowanie na incydenty

- Co zrobić, gdy podejrzewamy atak lub naruszenie danych.
- Kiedy i komu zgłaszać problem.
- Rola zespołu IT i procedur wewnętrznych.

9. Dobre praktyki i podsumowanie

- Dyskusja: „Co zrobiłbyś w tej sytuacji?”
- Podstawowe zasady cyberhigieny na co dzień.
- Jak rozwijać swoje nawyki bezpieczeństwa w pracy i w życiu prywatnym.
- Sesja pytań i odpowiedzi.

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	430,50 PLN
Koszt przypadający na 1 uczestnika netto	350,00 PLN
Koszt osobogodziny brutto	143,50 PLN
Koszt osobogodziny netto	116,67 PLN

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Tryb self-paced 24/7 – możliwość realizacji kursu w dowolnym czasie i miejscu, dostosowanie intensywności nauki do własnych potrzeb, brak barier geograficznych.

Platforma e-learningowa klasy SaaS – z funkcjami: ścieżki edukacyjne, analityka postępów, repozytorium materiałów, quizy, checklisty wdrożeniowe, pliki PDF, notatki cyfrowe, mikrospołeczność (komunikator), certyfikacja. Interaktywność

Zastosowanie multimedialnych materiałów (wideo, quizy, checklisty, ćwiczenia wdrożeniowe) zamiast tradycyjnych wykładów, co zwiększa zaangażowanie i efektywność nauki.

Warunki techniczne

Wymogi techniczne dla uczestników usługi

Do korzystania z Usługi Profesjonalnej Platformy Edukacyjnej e-LEA konieczne jest spełnienie następujących warunków technicznych przez komputer lub inne urządzenie Klienta lub Użytkownika Końcowego.

1. System operacyjny: Windows 7 lub nowszy, MacOS 10.12 lub nowszy.
2. 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.
3. Urządzenia peryferyjne lub wbudowane: słuchawki i mikrofon (lub głośniki i mikrofon), kamera internetowa – wymagane do udziału w wykładach LIVE.
4. Ekran: rozdzielczość co najmniej 1280x768.
5. Miejsce na dysku: 20 MB wolnego miejsca.
6. 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.

1. Rekomendowane parametry internetu: pobieranie i wysyłanie od 30 Mbps, opóźnienie do 40 ms.

2. Przeglądarka: aktualna wersja Chrome, Safari, Firefox lub Edge z obsługą plików audio i wideo.
3. Adres e-mail: aktywny adres e-mail uczestnika.
4. Urządzenia mobilne: aplikacja e-LEA pobrana z Google Play (Android) lub App Store (iOS).
5. Karta graficzna: opcjonalna, zwiększa płynność i wydajność przy dużej liczbie grafik i filmów.
6. Karta dźwiękowa: opcjonalna; w przypadku jej braku dźwięk odtwarzany jest przez urządzenia peryferyjne lub wbudowane.

Kontakt

MARIUSZ REJZEREWICZ

E-mail m.rejzerewicz@fu2res.eu

Telefon (+48) 579 044 794