Możliwość dofinansowania

Cyberbezpieczeństwo w praktyce dla firm

Numer usługi 2025/08/04/164038/2921656

2 000,00 PLN brutto
2 000,00 PLN netto
200,00 PLN brutto/h
200,00 PLN netto/h

LIFEPASS spółka z ograniczoną odpowiedzialnością

4,7 / 5

401 ocen

Kielce / stacjonarna
Usługa szkoleniowa
10 h
14.11.2025 do 14.11.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie skierowane jest do pracowników małych i średnich przedsiębiorstw, szczególnie z działów administracyjnych, sprzedaży, finansów oraz IT, którzy w codziennej pracy mają dostęp do danych wrażliwych lub systemów informatycznych. Uczestnicy nie muszą posiadać zaawansowanej wiedzy technicznej, jednak oczekiwane jest podstawowe obycie z komputerem i środowiskiem pracy biurowej. Grupa docelowa to osoby odpowiedzialne za przetwarzanie danych osobowych, komunikację mailową, korzystanie z aplikacji chmurowych oraz podstawowe bezpieczeństwo informacji w organizacji. Szkolenie jest odpowiednie zarówno dla pracowników z kilkuletnim doświadczeniem, jak i osób nowozatrudnionych, które chcą podnieść swoją świadomość w zakresie
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	13-11-2025
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	10
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Uczestnik szkolenia rozpozna i zinterpretuje zagrożenia cybernetyczne, zastosuje zasady ochrony danych osobowych i bezpiecznego korzystania z sieci. Będzie potrafił reagować na incydenty bezpieczeństwa, stosować procedury ochrony informacji i rozpoznawać próby phishingu. Po szkoleniu uczestnik świadomie i samodzielnie zadba o cyberbezpieczeństwo w środowisku pracy.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Definiuje podstawowe pojęcia związane z cyberbezpieczeństwem i zagrożeniami cyfrowymi w pracy biurowej.	Wymienia i charakteryzuje najczęstsze zagrożenia cybernetyczne (np. phishing, ransomware, socjotechnika).	Test teoretyczny
Charakteryzuje obowiązki prawne związane z ochroną danych osobowych w świetle RODO i krajowych regulacji.	Rozróżnia i omawia podstawy prawne przetwarzania danych osobowych w organizacji	Test teoretyczny
Rozpoznaje zagrożenia cybernetyczne w codziennym środowisku pracy.	Analizuje przykładowe sytuacje zagrożeń i klasyfikuje ich typ.	Obserwacja w warunkach symulowanych
Stosuje zasady bezpiecznego korzystania z urządzeń i systemów informatycznych.	Konfiguruje silne hasło, prawidłowo loguje się do systemów oraz stosuje dwuskładnikowe uwierzytelnianie.	Obserwacja w warunkach symulowanych
Przestrzega zasad odpowiedzialnego i etycznego postępowania z danymi i informacjami w organizacji.	Wskazuje właściwe zachowania w sytuacjach ryzyka naruszenia danych i komunikuje zagrożenie przełożonym.	Obserwacja w warunkach symulowanych

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

Tytuł szkolenia: Cyberbezpieczeństwo w praktyce dla firm

Forma świadczenia usługi: Stacjonarna

Czas trwania usługi: 10 godzin dydaktycznych (1godz=45 min)

Godziny realizacji: 09:00 do 16:30

Teoria: 5 godzin dydaktycznych

Praktyka: 3 godziny dydaktycznye

Przerwy: 2 godziny dydaktyczne wliczona w czas trwania usługi

Cele szkolenia:

Uczestnik szkolenia rozpozna i zinterpretuje zagrożenia cybernetyczne, zastosuje zasady ochrony danych osobowych i bezpiecznego korzystania z sieci. Będzie potrafił reagować na incydenty bezpieczeństwa, stosować procedury ochrony informacji i rozpoznawać próby phishingu. Po szkoleniu uczestnik świadomie i samodzielnie zadba o cyberbezpieczeństwo w środowisku pracy.

Grupa docelowa:

Szkolenie skierowane jest do pracowników małych i średnich przedsiębiorstw, szczególnie z działów administracyjnych, sprzedaży, finansów oraz IT, którzy w codziennej pracy mają dostęp do danych wrażliwych lub systemów informatycznych. Uczestnicy nie muszą posiadać zaawansowanej wiedzy technicznej, jednak oczekiwane jest podstawowe obycie z komputerem i środowiskiem pracy biurowej. Grupa docelowa to osoby odpowiedzialne za przetwarzanie danych osobowych, komunikację mailową, korzystanie z aplikacji chmurowych oraz podstawowe bezpieczeństwo informacji w organizacji. Szkolenie jest odpowiednie zarówno dla pracowników z kilkuletnim doświadczeniem, jak i osób nowozatrudnionych, które chcą podnieść swoją świadomość w zakresie

Liczba uczestników: max 15 osób

Trener i walidator:

W ramach realizacji usługi zachowany jest wyraźny podział ról trenera i walidatora, zgodnie z wymaganiami systemu BUR.

Trener odpowiada za przygotowanie i przeprowadzenie procesu edukacyjnego, w tym za wsparcie uczestników w osiąganiu założonych efektów uczenia się oraz za zebranie wymaganych dowodów i deklaracji uczestników.

Walidator nie uczestniczy w procesie szkoleniowym i nie wpływa na sposób przygotowania dokumentacji. Jego zadaniem jest niezależna ocena efektów uczenia się osiągniętych przez uczestników, na podstawie przekazanych materiałów. Ocena ta odbywa się zgodnie z przyjętymi standardami walidacji, przy zachowaniu pełnej neutralności i obiektywizmu

Zakres tematyczny szkolenia:

1. **Wprowadzenie i diagnoza wiedzy uczestników**

- Pre-test: rozpoznanie poziomu wiedzy uczestników z zakresu ochrony danych osobowych, cyberzagrożeń i dobrych praktyk.
- Zbieranie oczekiwań szkoleniowych.

2. **Ochrona danych osobowych i podstawy prawne**

- Wprowadzenie do ochrony danych osobowych w MŚP.
- Regulacje RODO:
  - Kluczowe pojęcia i definicje.
  - Obowiązki administratora danych.
- Podstawy prawne przetwarzania danych:
  - Zgody, umowy powierzenia, rejestr czynności.
- Ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC).

- Dyrektywa NIS2 i jej wymogi dla MŚP.
- Sankcje i kary.
- Przykłady błędów i naruszeń (case studies).

3. **Praktyczne aspekty RODO**

- Typowe naruszenia danych: ransomware, phishing, wycieki danych.
- Konsekwencje prawne.
- Procedury zgłaszania incydentów.
- Dobre praktyki w ochronie danych.

4. **Cyberzagrożenia: przykłady ataków i rekonstrukcja**

- Analiza realnych ataków na firmy i osoby:
  - Phishing, BEC (Business Email Compromise), ransomware.
  - Ataki na aplikacje webowe i mobilne.
- Przebieg ataku: wektory, działania atakujących.
- Studium przypadków i rekonstrukcja incydentów.

5. **Cyberhigiena i codzienne bezpieczeństwo**

- Zarządzanie hasłami.
- Uwierzytelnianie wieloskładnikowe (MFA).
- Tworzenie i przechowywanie kopii zapasowych (backup).
- Segmentacja sieci i ograniczanie uprawnień.
- Szkolenia pracowników.

6. **Socjotechnika i manipulacje**

- Techniki inżynierii społecznej: phishing, vishing.
- Rozpoznawanie prób manipulacji i oszustw.
- Symulacje rozmów (ćwiczenia praktyczne).

7. **Reagowanie na incydenty i ciągłość działania**

- Procedury reagowania na incydenty.
- Komunikacja z zespołem i klientami.
- Dokumentacja incydentów.
- Planowanie awaryjne.
- Studium przypadków i ćwiczenia praktyczne.

8. Walidacja usługi

Metody pracy:

- Prezentacja multimedialna
- Ćwiczenia praktyczne
- Symulacje i analiza przypadków
- Konsultacje indywidualne i grupowe

Weryfikacja efektów uczenia się:

- Test wiedzy (pre- i post-test)
- Feedback od prowadzącego
- Test walidacyjny
- Ankieta ewaluacyjna

Harmonogram

Liczba przedmiotów/zajęć: 11

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 11 Diagnoza wiedzy, oczekiwań i potrzeb uczestników.	Katarzyna Brodnicka	14-11-2025	09:00	09:20	00:20
2 z 11 Ochrona danych osobowych – RODO, KSC, NIS2, obowiązki, podstawy prawne, najczęstsze błędy.	Katarzyna Brodnicka	14-11-2025	09:20	10:40	01:20
3 z 11 Praktyka RODO – przykłady naruszeń, konsekwencje, dobre praktyki i procedury zgłaszania.	Katarzyna Brodnicka	14-11-2025	10:40	11:40	01:00
4 z 11 Przerwa	Katarzyna Brodnicka	14-11-2025	11:40	11:50	00:10
5 z 11 Realne ataki – analiza phishingu, ransomware, BEC, rekonstrukcja incydentów.	Katarzyna Brodnicka	14-11-2025	11:50	13:00	01:10
6 z 11 Przerwa obiadowa	Katarzyna Brodnicka	14-11-2025	13:00	13:30	00:30
7 z 11 Cyberhigiena – hasła, MFA, backupy, segmentacja, ograniczenia, szkolenia.	Katarzyna Brodnicka	14-11-2025	13:30	14:00	00:30
8 z 11 Socjotechnika – techniki manipulacji, phishing, vishing, ćwiczenia praktyczne.	Katarzyna Brodnicka	14-11-2025	14:00	14:40	00:40

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
9 z 11 Przerwa	Katarzyna Brodnicka	14-11-2025	14:40	14:50	00:10
10 z 11 Reagowanie na incydenty – komunikacja, dokumentacja, ćwiczenia, planowanie ciągłości.	Katarzyna Brodnicka	14-11-2025	14:50	16:00	01:10
11 z 11 Walidacja usługi	-	14-11-2025	16:00	16:30	00:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 000,00 PLN
Koszt przypadający na 1 uczestnika netto	2 000,00 PLN
Koszt osobogodziny brutto	200,00 PLN
Koszt osobogodziny netto	200,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Katarzyna Brodnicka

Katarzyna Brodnicka to doświadczona ekspertka w dziedzinie bezpieczeństwa informacji, ochrony danych oraz cyberbezpieczeństwa. Posiada bogate doświadczenie zawodowe, które zdobywała w różnych instytucjach, m.in. jako Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z normą ISO 27001:2022, a także jako Inspektor Ochrony Danych (IOD). W ramach swojej kariery zawodowej, Katarzyna specjalizuje się w prowadzeniu audytów, zarządzaniu ryzykiem oraz wdrażaniu polityk bezpieczeństwa zarówno w administracji, jak i w sektorze prywatnym. Ponadto zajmuje się opracowywaniem dokumentacji technicznych, wdrażaniem rozwiązań technologicznych i prowadzeniem szkoleń z zakresu cyberbezpieczeństwa zarówno dla kadry zarządzającej, jak i zespołów technicznych. Prowadzi również własną Kancelarię Audytorską

"KB Brand," oferując wsparcie w zakresie audytów, szkoleń oraz wdrażania polityk bezpieczeństwa. Jest ceniona za profesjonalizm, szeroką wiedzę oraz umiejętność dostosowywania metod szkoleniowych do specyficznych potrzeb klientów.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy uczestnik szkolenia otrzymuje kompletny skrypt szkoleniowy zawierający najważniejsze informacje i materiały omawiane podczas zajęć.

Warunki uczestnictwa

Niezbędnym warunkiem uczestnictwa w szkoleniach i doradztwie, które dofinansowane są z funduszy europejskich jest założenie konta indywidualnego, a później firmowego w Bazie Usług Rozwojowych. Następnie zapis na wybrane szkolenie za pośrednictwem Bazy Usług Rozwojowych, spełnienie warunków przedstawionych przez danego Operatora, który dysponuje funduszami. Złożenie dokumentów o dofinansowanie do usługi rozwojowej u Operatora Usługi, zgodnie z wymogami jakie określił.

Ponadto niezbędnym warunkiem do nabycia kompetencji jest pełnoletność, wykształcenie co najmniej średnie, wypełnienie testu wiedzy lub odbycie rozmowy kwalifikacyjnej przed i po szkoleniu

Informacje dodatkowe

Planujemy dwie 10 minutowe przerwy pomiędzy modułami oraz jedną 30 minutową obiadową. Usługa jest zwolniona z podatku VAT w przypadku, kiedy przedsiębiorstwo zwolnione jest z podatku VAT lub dofinansowanie wynosi co najmniej 70%.W innej sytuacji do ceny netto doliczany jest podatek VAT w wysokości 23%.Podstawa: §3 ust. 1 pkt. 14 rozporządzenia Ministra Finansów z dnia 20.12.2013 r. w sprawie zwolnień od podatku od towarów i usług oraz szczegółowych warunków stosowania tych zwolnień (Dz.U. z 2018 r., poz. 701).

Warunkiem zaliczenia jest napisanie pre i post testów oraz testu walidacyjnego.

Uczestnictwo w min. 80% zajęć liczone na podstawie listy obecności w każdym dniu szkolenia.

Uczestnicy są świadomi, że usługa realizowana z dofinansowaniem może podlegać monitoringowi ze strony Operatora lub PARP i wyrażają zgodę na jego przeprowadzenie.

Uczestnik otrzyma zaświadczenie ze szkolenia.

Adres

ul. 1 Maja 191
25-646 Kielce
woj. świętokrzyskie

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi

Kontakt

Lucyna Kuchta

E-mail kontakt@edumeo.pl
Telefon (+48) 577 203 338