Możliwość dofinansowania

Cyberbezpieczeństwo w codziennej pracy – szkolenie praktyczne

Numer usługi 2025/11/17/164038/3152098

750,00 PLN brutto
750,00 PLN netto
93,75 PLN brutto/h
93,75 PLN netto/h

LIFEPASS spółka z ograniczoną odpowiedzialnością

4,7 / 5

530 ocen

zdalna w czasie rzeczywistym
Usługa szkoleniowa
8 h
05.02.2026 do 05.02.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Usługa szkoleniowa jest skierowana do wszystkich pracowników jednostek samorządu terytorialnego i przedsiębiorstw, którzy w codziennej pracy korzystają z komputera, poczty elektronicznej, systemów informatycznych lub przetwarzają informacje służbowe. Są to m.in. pracownicy administracyjni, biurowi, techniczni, obsługujący dokumentację, komunikację wewnętrzną oraz podstawowe narzędzia cyfrowe. Do grupy należą osoby o różnym poziomie doświadczenia – zarówno pracownicy początkujący, jak i wieloletni użytkownicy systemów IT, którzy nie pełnią jednak funkcji specjalistycznych w obszarze bezpieczeństwa informacji. Uczestnicy powinni wykonywać zadania związane z obiegiem dokumentów, kontaktami e-mailowymi, pracą na danych oraz obsługą systemów organizacyjnych, gdzie kluczowe jest przestrzeganie zasad cyberbezpieczeństwa i właściwe reagowanie na zagrożenia. Szkolenie kierowane jest do osób chcących zwiększyć świadomość zagrożeń oraz rozwijać kompetencje bezpiecznej pracy w środowisku cyfrowym.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	04-02-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	8
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Uczestnik po zakończeniu szkolenia będzie rozpoznawał zagrożenia cyberbezpieczeństwa, stosował zasady ochrony informacji oraz bezpiecznej pracy z danymi, tworzył i wykorzystywał silne hasła oraz uwierzytelnianie 2FA, analizował i oceniał ryzykowne sytuacje, a także reagował na incydenty bezpieczeństwa i zgłaszał je zgodnie z procedurami obowiązującymi w organizacji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik definiuje podstawowe pojęcia i zasady bezpieczeństwa informacji.	Uczestnik rozróżnia kluczowe pojęcia związane z bezpieczeństwem informacji (poufność, integralność, dostępność).	Test teoretyczny
	Uczestnik klasyfikuje podstawowe zagrożenia cyberbezpieczeństwa i ich źródła.	Test teoretyczny
Uczestnik charakteryzuje wymagania prawne i organizacyjne dotyczące bezpieczeństwa informacji.	Uczestnik opisuje obowiązki pracownika wynikające z KRI, uoKSC i RODO	Test teoretyczny
	Uczestnik identyfikuje elementy organizacyjnych zasad bezpieczeństwa, w tym procedury reagowania na incydenty.	Test teoretyczny
Uczestnik analizuje ryzykowne sytuacje i rozpoznaje próby ataków socjotechnicznych.	Uczestnik wskazuje elementy świadczące o potencjalnym phishingu na przykładach wiadomości i stron.	Obserwacja w warunkach symulowanych
	Uczestnik ocenia, czy dane zachowanie użytkownika stanowi ryzyko dla bezpieczeństwa informacji.	Obserwacja w warunkach symulowanych
Uczestnik tworzy bezpieczne hasło zgodne z zasadami organizacji i stosuje 2FA w zadaniu symulowanym.	Uczestnik uzasadnia konieczność stosowania ustalonych procedur bezpieczeństwa w codziennych działaniach.	Obserwacja w warunkach symulowanych
	Uczestnik deklaruje gotowość współpracy z przełożonymi i zespołem przy zgłaszaniu incydentów.	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: Cyberbezpieczeństwo w codziennej pracy – szkolenie praktyczne

Forma świadczenia usługi: zdalna w czasie rzeczywistym

Czas trwania usługi: 8 godzin dydaktycznych

Godziny realizacji: 8:30 do 14:30

Teoria: 4 godziny dydaktyczne

Praktyka: 3 godziny dydaktyczne

Przerwy: 1 godzina dydaktyczna wliczona w czas szkolenia

Cele szkolenia:

Uczestnik po zakończeniu szkolenia będzie rozpoznawał zagrożenia cyberbezpieczeństwa, stosował zasady ochrony informacji oraz bezpiecznej pracy z danymi, tworzył i wykorzystywał silne hasła oraz uwierzytelnianie 2FA, analizował i oceniał ryzykowne sytuacje, a także reagował na incydenty bezpieczeństwa i zgłaszał je zgodnie z procedurami obowiązującymi w organizacji.

Grupa docelowa:

Usługa szkoleniowa jest skierowana do wszystkich pracowników jednostek samorządu terytorialnego i przedsiębiorstw, którzy w codziennej pracy korzystają z komputera, poczty elektronicznej, systemów informatycznych lub przetwarzają informacje służbowe. Są to m.in. pracownicy administracyjni, biurowi, techniczni, obsługujący dokumentację, komunikację wewnętrzną oraz podstawowe narzędzia cyfrowe. Do grupy należą osoby o różnym poziomie doświadczenia – zarówno pracownicy początkujący, jak i wieloletni użytkownicy systemów IT, którzy nie pełnią jednak funkcji specjalistycznych w obszarze bezpieczeństwa informacji. Uczestnicy powinni wykonywać zadania związane z obiegiem dokumentów, kontaktami e-mailowymi, pracą na danych oraz obsługą systemów organizacyjnych, gdzie kluczowe jest przestrzeganie zasad cyberbezpieczeństwa i właściwe reagowanie na zagrożenia. Szkolenie kierowane jest do osób chcących zwiększyć świadomość zagrożeń oraz rozwijać kompetencje bezpiecznej pracy w środowisku cyfrowym.

Liczba osób: max 20 uczestników

Terener 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:

Podstawy bezpieczeństwa informacji

- kluczowe pojęcia i definicje
- standardy i regulacje dotyczące bezpieczeństwa
- polityki i procedury bezpieczeństwa w organizacji
- obowiązki pracownika wynikające z KRI, uoKSC i RODO
- rola pracownika w Systemie Zarządzania Bezpieczeństwem Informacji

Najczęstsze zagrożenia w środowisku cyfrowym

- błędy użytkowników jako główna przyczyna incydentów
- socjotechniki (phishing, vishing, smishing)
- oszustwa typu BEC
- malware: ransomware, trojany, spyware
- rozpoznawanie podejrzanych wiadomości, linków i załączników

Ochrona informacji w praktyce

- zasady bezpiecznej pracy z danymi
- poufność stanowiska pracy (ekran, dokumenty, rozmowy)
- tworzenie i stosowanie silnych haseł
- uwierzytelnienie dwuskładnikowe (2FA)
- przechowywanie i niszczenie dokumentów
- zabezpieczenia fizyczne i organizacyjne

Reagowanie na incydenty bezpieczeństwa

- rodzaje incydentów i ich symptomy
- pierwsze kroki po podejrzeniu incydentu
- zgłaszanie incydentów zgodnie z procedurami organizacji
- zachowania minimalizujące szkody
- przykłady realnych incydentów i analiza działań

Walidacja usługi

Metody szkoleniowe:

- Wykłady teoretyczne.
- Prezentacja
- Ćwiczenia praktyczne
- Konsultacje indywidualne i grupowe
- Dyskusje grupowe: Rozwiązywanie problemów i analiza przypadków.

Weryfikacja efektów uczenia się:

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

Harmonogram

Liczba przedmiotów/zajęć: 9

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 9 Powitanie uczestników, przedstawienie zasad i celów szkolenia oraz krótkie omówienie znaczenia bezpieczeństwa informacji w codziennej pracy.	Stanisław Chyb	05-02-2026	08:30	08:45	00:15
2 z 9 Bezpieczeństwo informacji – podstawy Omówienie kluczowych pojęć, standardów, procedur organizacyjnych, obowiązków z KRI uoKSC i RODO oraz roli pracownika w SZBI z krótkim ćwiczeniem sytuacyjnym.	Stanisław Chyb	05-02-2026	08:45	09:45	01:00
3 z 9 Przerwa	Stanisław Chyb	05-02-2026	09:45	10:00	00:15
4 z 9 Najczęstsze zagrożenia w pracy Przedstawienie błędów użytkowników, metod socjotechniki, oszustw BEC oraz rozpoznawania podejrzanych e-maili z analizą realnych przykładów i ćwiczeniami.	Stanisław Chyb	05-02-2026	10:00	11:15	01:15
5 z 9 Przerwa	Stanisław Chyb	05-02-2026	11:15	11:30	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
6 z 9 Zasady bezpiecznej pracy z danymi, ochrona stanowiska, tworzenie silnych haseł, stosowanie 2FA, prawidłowe przechowywanie i niszczenie dokumentów oraz odpowiedzialność pracownika.	Stanisław Chyb	05-02-2026	11:30	12:45	01:15
7 z 9 Przerwa	Stanisław Chyb	05-02-2026	12:45	13:00	00:15
8 z 9 Reagowanie na incydenty Wyjaśnienie czym jest incydent bezpieczeństwa, jak go rozpoznać i zgłosić, jakie działania podjąć po kliknięciu w podejrzany link oraz ćwiczenie procedury zgłaszania.	Stanisław Chyb	05-02-2026	13:00	14:00	01:00
9 z 9 Walidacja usługi	Stanisław Chyb	05-02-2026	14:00	14:30	00:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	750,00 PLN
Koszt przypadający na 1 uczestnika netto	750,00 PLN
Koszt osobogodziny brutto	93,75 PLN
Koszt osobogodziny netto	93,75 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Stanisław Chyb

Oficer Wojska Polskiego od 2012 r. w czynnej służbie. Absolwent Wojskowej Akademii Technicznej w Warszawie, Uniwersytetu Ekonomicznego we Wrocławiu oraz Wyższej Szkoły Biznesu – National Louis University z siedzibą w Nowym Sączu. Specjalista w zakresie łączności, teleinformatyki, cyberbezpieczeństwa i kryptografii oraz szeroko pojętego zarządzania (ZZL, technologią, procesami i projektami). Instruktor survivalowych kursów przygotowawczych obejmujących elementy S.E.R.E. Podczas 13-letniej praktyki zawodowej zajmował stanowiska kierownicze zarówno w strukturach krajowych, jak i międzynarodowych, skutecznie przekazując wiedzę podwładnym i współpracownikom. Posiada bogate doświadczenie zawodowe potwierdzone wyróżnieniami w zakresie bezpieczeństwa, organizacji i eksploatacji systemów łączności i informatyki, a także zarządzania projektami i procesami oraz przywództwa. Auditor wiodący Systemów Zarządzania Bezpieczeństwem Informacji ISO/IEC 27001.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy uczestnik szkolenia otrzymuje kompletny skrypt szkoleniowy w pdf 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 trzy 15 minutowe przerwy pomiędzy modułami. 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.

Warunki techniczne

Warunki techniczne

- Procesor dwurdzeniowy 2GHz lub lepszy (zalecany czterordzeniowy);
- 2GB pamięci RAM (zalecane 4GB lub więcej);
- System operacyjny taki jak Windows 8 (zalecany Windows 10), Mac OS wersja 10.13 (zalecana najnowsza wersja), Linux, łącze internetowe – min. 5mb/s
- Przeglądarka internetowa – Chrome, Firefox lub Microsoft Edge. W przypadku Mac OS – Safari
- Aby móc korzystać z usługi na niektórych urządzeniach mobilnych, konieczne może być pobranie odpowiedniej aplikacji w iTunes App Store lub Google Play Store. Do korzystania z usługi w pełnym zakresie dźwięku i obrazu podczas konferencji, konieczne jest posiadanie, mikrofonu lub zestawu słuchawkowego, lub głośników podłączonych do urządzenia i rozpoznanych przez Państwa urządzenie i nie powinny być one jednocześnie używane przez żadną inną aplikację.
- Uczestnik musi mieć zapewniony sprzęt komputerowy we własnym zakresie z dostępem do kamery i mikrofonu.

Kontakt

Lucyna Kuchta

E-mail kontakt@edumeo.pl

Telefon (+48) 577 203 338