Możliwość dofinansowania

Cyberbezpieczeństwo i ochrona danych osobistych w przedsiębiorstwie - szkolenie.

Numer usługi 2025/10/28/174663/3110386
ADVERT Edyta Stąpór-Rynk
4,8 / 5
189 ocen
2 880,00 PLN
brutto
2 880,00 PLN
netto
180,00 PLN
brutto/h
180,00 PLN
netto/h
zdalna w czasie rzeczywistym
Usługa szkoleniowa
16 h
16.02.2026 do 17.02.2026

Informacje podstawowe

- Kategoria
  Informatyka i telekomunikacja / Bezpieczeństwo IT
- Grupa docelowa usługi

  Szkolenie przeznaczone dla przedsiębiorców i ich pracowników, którzy chcą poznać zasady ochrony przed cyberprzestępczością, oraz z uwagi na fakt zarządzania danymi osobowymi, ochrony tych danych przed atakami hakerów. Szkolenie dedykowane dla kadry zarządzającej, menagerów, księgowych, kancelarii prawnych.

  Szkolenie jest dostępne dla wszystkich zainteresowanych - bez względu na poziom doświadczenia w danej dziedzinie. Wierzymy, że każdy uczestnik będzie miał okazję pogłębić swoją wiedzę.

- Minimalna liczba uczestników
  2
- Maksymalna liczba uczestników
  25
- Data zakończenia rekrutacji
  08-02-2026
- Forma prowadzenia usługi
  zdalna w czasie rzeczywistym
- Liczba godzin usługi
  16
- Podstawa uzyskania wpisu do BUR
  Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Usługa ,, Cyberbezpieczeństwo i ochrona danych osobistych w przedsiębiorstwie."
Przygotowuje uczestników do nabycia wiedzy oraz umiejętności praktycznych dotyczących ochrony przed atakami cyberprzestępców, wirusami, złośliwym oprogramowaniem.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się, kryteria weryfikacji i metody walidacji.

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Efekty uczenia się W ZAKRESIE WIEDZY: Posiada wiedzę z zakresu zagrożeń cyberbezpieczeństwa i metod ochrony danych osobistych.	Kryteria weryfikacji rozróżnia rodzaje zagrożeń w cyberprzestrzeni (np. phishing, malware, ransomware, spyware),	Metoda walidacji Test teoretyczny
	Kryteria weryfikacji • charakteryzuje sposoby ataków na systemy operacyjne i sieci komputerowe,	Metoda walidacji Test teoretyczny
	Kryteria weryfikacji • omawia zasady bezpiecznego korzystania z Internetu, poczty e-mail, chmury i mediów społecznościowych,	Metoda walidacji Test teoretyczny
	Kryteria weryfikacji • wskazuje narzędzia i technologie stosowane do ochrony danych (np. firewalle, programy antywirusowe, VPN),	Metoda walidacji Test teoretyczny
	Kryteria weryfikacji • opisuje zasady działania metod socjotechnicznych i ich wpływ na bezpieczeństwo informacji	Metoda walidacji Test teoretyczny
	Kryteria weryfikacji • konfiguruje przeglądarkę w trybie prywatnym/incognito i usuwa ślady aktywności w sieci,	Metoda walidacji Test teoretyczny
	Kryteria weryfikacji • tworzy i przywraca kopie zapasowe danych,	Metoda walidacji Test teoretyczny
Efekty uczenia się W ZAKRESIE UMIEJĘTNOŚCI Monitoruje i stosuje zasady bezpiecznego korzystania z zasobów sieciowych oraz chroni dane osobowe w praktyce.	Kryteria weryfikacji • identyfikuje sytuacje zwiększonego ryzyka wycieku danych osobowych,	Metoda walidacji Test teoretyczny
	Kryteria weryfikacji • stosuje metody bezpiecznego logowania i uwierzytelniania użytkowników,	Metoda walidacji Test teoretyczny
	Kryteria weryfikacji • posługuje się narzędziami do szyfrowania i zabezpieczania plików oraz folderów.	Metoda walidacji Test teoretyczny
Efekty uczenia się W ZAKRESIE KOMPETENCJI SPOŁECZNYCH : Stosuje zasady odpowiedzialnego i świadomego zachowania w	Kryteria weryfikacji rozpoznaje próby wyłudzenia danych i fałszywe komunikaty (np. fałszywe e-maile, linki, aplikacje),	Metoda walidacji Obserwacja w warunkach rzeczywistych

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
środowisku cyfrowym.	Kryteria weryfikacji • odróżnia legalne działania od nieetycznych praktyk w sieci,	Metoda walidacji Obserwacja w warunkach rzeczywistych
	Kryteria weryfikacji • definiuje i omawia pojęcia związane z cyberbezpieczeństwem (np. VPN, trojan, malware, szyfrowanie, incydent bezpieczeństwa),	Metoda walidacji Obserwacja w warunkach rzeczywistych
	Kryteria weryfikacji • wykazuje postawę odpowiedzialności za ochronę danych w środowisku pracy,	Metoda walidacji Obserwacja w warunkach rzeczywistych
	Kryteria weryfikacji • komunikuje zagrożenia cyfrowe współpracownikom i wspiera ich w stosowaniu zasad bezpieczeństwa.	Metoda walidacji 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

1 – Część teoretyczna:

• Jak dbać o swoją tożsamość cyfrową. Wirusy, szpiegowanie, rodzaje, sposoby hakowania. Tryb bezpieczny, monitorowanie zachowań w sieci. Rodzaje oraz narzędzia wykorzystywane do ataków hakerskich.

• Zarządzanie i ochrona danych w przedsiębiorstwie e- szyfrowanie danych – kopie bezpieczeństwa - ochrona danych osobowych klientów - po ataku - studium przypadków -incydenty bezpieczeństwa.

2 – Część praktyczna:

• Jak dbać o swoją tożsamość cyfrową. Wirusy, szpiegowanie, rodzaje, sposoby hakowania. Tryb bezpieczny, monitorowanie zachowań w sieci. Rodzaje oraz narzędzia wykorzystywane do ataków hakerskich.

• Zarządzanie i ochrona danych w przedsiębiorstwie e- szyfrowanie danych – kopie bezpieczeństwa - ochrona danych osobowych klientów - po ataku - studium przypadków -incydenty bezpieczeństwa.

• Walidacja

Szkolenie kierowane jest do wszystkich osób zainteresowanych tematyką, niezależnie od poziomu dotychczasowego doświadczenia czy wiedzy w tej dziedzinie. Szkolenie zostało przygotowane w taki sposób, aby każdy uczestnik – zarówno początkujący, jak i bardziej zaawansowany – miał możliwość rozwinięcia swoich kompetencji oraz poszerzenia wiedzy zgodnie z własnymi potrzebami i oczekiwaniami.

Warunki organizacyjne: każdy uczestnik pracuje indywidualnie przy samodzielnym stanowisku komputerowym.

W harmonogramie uwzględniono godziny zegarowe, natomiast kurs opiera się na 45-minutowych godzinach dydaktycznych- stąd rozbieżność pomiędzy liczbą godzin w harmonogramie a ogólną liczbą godzin kursu.

1 godzina= 45 minut (godzina szkoleniowa)

Szkolenie obejmuje łącznie 16 godzin dydaktycznych, co przekłada się na 12 godzin zegarowych. Szkolenie obejmuje 1:30 przerwy. 12 godzin dydaktycznych to część teoretyczna zaś 4 godziny dydaktyczne obejmuje część praktyczna. Podczas ostatnich 30 minut szkolenia zostanie przeprowadzona walidacja.

Przerwy nie są wliczane w czas szkolenia.

Walidacja

Ostatnie 30 minut szkolenia zostało przeznaczone na walidację w formie obserwacji w warunkach rzeczywistych. W tym czasie uczestnicy pracują z przygotowaną prezentacją, w której znajduje się 5 praktycznych zadań związanych z tematyką szkolenia. Każde zadanie wymaga wykonania określonej czynności lub udzielenia poprawnej odpowiedzi. Uczestnicy wpisują swoje rozwiązania bezpośrednio na czacie platformy, co umożliwia walidatorowi bieżące monitorowanie, ocenę poprawności odpowiedzi oraz potwierdzenie osiągnięcia zakładanych efektów uczenia się.

Walidatorem jest Aleksandra Kozak

Szkolenie będzie realizowane w formie zdalnej za pomocą platformy ClickMeeting.

Całość nagrania zostanie zarchiwizowana i umieszczona na dysku zewnętrznym w celu kontroli i audytu.

1. Prezentacja powerpoint celem utrwalenia informacji przekazanych w trakcie szkolenia drogą mailową.

2. E-materiały w formacie PDF.

Szkolenie w formie zdalnej będzie odbywało się w czasie rzeczywistym. W zależności od czasu potrzeb będą wykorzystywane różne elementy: ćwiczenia, testy, ankiety, udostępnianie ekranu i inne. Całe szkolenie jest rejestrowane w celach kontroli/audytu. Wykorzystanie nagrania w innym celu niż kontrola/audyt wymaga zgody Trenera i Uczestników

Harmonogram

Liczba przedmiotów/zajęć: 15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 15 Ochrona tożsamości cyfrowej; wirusy i szpiegowanie — rodzaje i metody hakowania; tryb bezpieczny i monitorowanie aktywności online; narzędzia stosowane w atakach hakerskich. Pre-test Wykład	Rafał Tomaszewski	16-02-2026	09:00	10:30	01:30
2 z 15 przerwa	Rafał Tomaszewski	16-02-2026	10:30	10:45	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
3 z 15 Ochrona tożsamości cyfrowej; wirusy i szpiegowanie — rodzaje i metody hakowania; tryb bezpieczny i monitorowanie aktywności online; narzędzia stosowane w atakach hakerskich. Ćwiczenia, test	Rafał Tomaszewski	16-02-2026	10:45	12:15	01:30
4 z 15 przerwa	Rafał Tomaszewski	16-02-2026	12:15	12:30	00:15
5 z 15 Ochrona tożsamości cyfrowej; wirusy i szpiegowanie — rodzaje i metody hakowania; tryb bezpieczny i monitorowanie aktywności online; narzędzia stosowane w atakach hakerskich. Chat	Rafał Tomaszewski	16-02-2026	12:30	14:00	01:30
6 z 15 przerwa	Rafał Tomaszewski	16-02-2026	14:00	14:15	00:15
7 z 15 Ochrona tożsamości cyfrowej; wirusy i szpiegowanie — rodzaje i metody hakowania; tryb bezpieczny i monitorowanie aktywności online; narzędzia stosowane w atakach hakerskich. Ćwiczenia, test	Rafał Tomaszewski	16-02-2026	14:15	15:45	01:30
8 z 15 Zarządzanie i ochrona danych w przedsiębiorstwie- szyfrowanie danych - kopie bezpieczeństwa - ochrona danych osobowych klientów - po ataku - studium przypadków - incydenty bezpieczeństwa. Wykład	Rafał Tomaszewski	17-02-2026	09:00	10:30	01:30
9 z 15 przerwa	Rafał Tomaszewski	17-02-2026	10:30	10:45	00:15
10 z 15 Zarządzanie i ochrona danych w przedsiębiorstwie- szyfrowanie danych - kopie bezpieczeństwa - ochrona danych osobowych klientów - po ataku - studium przypadków - incydenty bezpieczeństwa. ćwiczenia	Rafał Tomaszewski	17-02-2026	10:45	12:15	01:30
11 z 15 przerwa	Rafał Tomaszewski	17-02-2026	12:15	12:30	00:15
12 z 15 Zarządzanie i ochrona danych w przedsiębiorstwie- szyfrowanie danych - kopie bezpieczeństwa - ochrona danych osobowych klientów - po ataku - studium przypadków - incydenty bezpieczeństw. Chat	Rafał Tomaszewski	17-02-2026	12:30	14:00	01:30
13 z 15 przerwa	Rafał Tomaszewski	17-02-2026	14:00	14:15	00:15
14 z 15 Zarządzanie i ochrona danych w przedsiębiorstwie- szyfrowanie danych - kopie bezpieczeństwa - ochrona danych osobowych klientów - po ataku - studium przypadków - incydenty bezpieczeństwa. Test	Rafał Tomaszewski	17-02-2026	14:15	15:15	01:00
15 z 15 Post- test. Walidacja w formie obserwacji w warunkach rzeczywistych.	-	17-02-2026	15:15	15:45	00:30

Cennik

Cennik

- Rodzaj ceny
  Cena
- Koszt przypadający na 1 uczestnika brutto
  2 880,00 PLN
- Koszt przypadający na 1 uczestnika netto
  2 880,00 PLN
- Koszt osobogodziny brutto
  180,00 PLN
- Koszt osobogodziny netto
  180,00 PLN

Prowadzący

Liczba prowadzących: 1
1 z 1

Rafał Tomaszewski

Rafał Tomaszewski to doświadczony trener, który od lat specjalizuje się w wspieraniu przedsiębiorców w prowadzeniu działalności gospodarczej. Jego wszechstronne wykształcenie oraz bogate doświadczenie zawodowe stanowią solidną podstawę dla oferowanych przez niego usług. Posiadając wykształcenie wyższe ekonomiczne, ze specjalnością w rachunkowości, Rafał Tomaszewski rozpoczął swoją karierę zawodową w 2010 roku. Od tego czasu aktywnie wykorzystuje swoją wiedzę i umiejętności w obszarze zarządzania finansami oraz prowadzenia rachunkowości w firmach. Aktualnie, jest certyfikowanym Audytorem Wiodącym Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z normą ISO 27001, co świadczy o jego zaawansowanych umiejętnościach w zakresie zarządzania ryzykiem i ochrony informacji w firmach. Ponadto, jest absolwentem studiów podyplomowych z zakresu Zarządzania Cyberbezpieczeństwem, co dodatkowo podkreśla jego specjalizację w obszarze bezpieczeństwa IT. Rafał Tomaszewski wyróżnia się profesjonalizmem, zaangażowaniem oraz umiejętnością dostosowywania się do zmieniających się warunków rynkowych i technologicznych. Jego głównym celem jest pomaganie przedsiębiorcom w osiągnięciu sukcesu poprzez efektywne zarządzanie finansami, procesami oraz bezpieczeństwem informacji.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymają nagranie ze szkolenia oraz prezentację Power Point przygotowane przez Trenera wysłane na adres e-mail.

Warunki uczestnictwa

Warunkiem uczestnictwa jest zarejestrowanie się i założenie konta w Bazie Usług Rozwojowych, zapisanie się na szkolenie za pośrednictwem Bazy oraz spełnienie wszystkich warunków określonych przez Operatora, do którego składają Panstwo dokumenty o dofinansowanie.

Przed podpisaniem umowy o dofinansowanie szkolenia z Operatorem, skontaktuj się z nami w celu potwierdzenia terminu szkolenia i dostępności wolnych miejsc. Informujemy, że w trakcie szkolenia możliwa jest wizytacja z udziałem PARP, Operatora lub innej jednostki wyznaczonej w celu sprawdzenia poprawności realizacji usługi.

Szkolenie w formie zdalnej będzie odbywało się w czasie rzeczywistym. W zależności od czasu potrzeb będą wykorzystywane różne elementy: ćwiczenia, testy, ankiety, udostępnianie ekranu i inne.

Informacje dodatkowe

Uwaga:

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).

Całe szkolenie jest rejestrowane w celach kontroli/audytu. Wykorzystanie nagrania w innym celu niż kontrola/audyt wymaga zgody Trenera i Uczestników.

Uczestnicy otrzymają zaświadczenie, potwierdzające że ukończyli szkolenie.

Forma świadczenia usługi :

Zdalna w czasie rzeczywistym - prowadzona na żywo.

Warunki techniczne

Wymagania, które muszą zostać spełnione, aby uczestniczyć w szkoleniu na ClickMeeting.:

- 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, Chrome OS.

Ponieważ ClickMeeting jest platformą opartą na przeglądarce, wymagane jest korzystanie z najaktualniejszych oficjalnych wersji Google Chrome, Mozilla Firefox, Safari, Edge lub Opera.

ClickMeeting współpracuje z wszystkimi wbudowanymi w laptopy kamerami oraz większością kamer internetowych. Bardziej zaawansowana lub profesjonalna kamera może wymagać instalacji dodatkowego oprogramowania lub sprzętu.

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 zestawu słuchawkowego, lub głośników podłączonych do urządzenia i rozpoznanych przez Państwa urządzenie i nie powinny być one jednocześnie używane przez żadną inną aplikację.

Okres ważności linku: Link będzie ważny w dniach i godzinach wskazanych w harmonogramie usługi.

Metody pracy podczas szkolenia on-line:

- wygodna forma szkolenia - wystarczy dostęp do urządzenia z internetem (komputer, tablet, telefon), słuchawki lub głośniki

- szkolenie realizowane jest w nowoczesnej formie w wirtualnym pokoju konferencyjnym i kameralnej grupie uczestników

- bierzesz udział w pełnowartościowym szkoleniu - Trener prowadzi zajęcia "na żywo" - widzisz go i słyszysz

- pokaz prezentacji, ankiet i ćwiczeń widzisz na ekranie swojego komputera w czasie rzeczywistym.

Kontakt

ALEKSANDRA KOZAK

E-mail
a.jonca@fpd.pl
Telefon
(+48) 574 157 925