Możliwość dofinansowania

Cyberbezpieczeństwo i ochrona danych osobistych i przedsiębiorstwie.

Numer usługi 2024/05/16/51161/2151866

2 730,00 PLN brutto
2 730,00 PLN netto
170,63 PLN brutto/h
170,63 PLN netto/h

FPD spółka z ograniczoną odpowiedzialnością

★★★★★

zdalna w czasie rzeczywistym
Usługa szkoleniowa
16 h
24.07.2024 do 25.07.2024

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Szkolenie przeznaczone dla przedsiebiorców 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 zarządzajacej, 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	8
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	23-07-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
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

Celem szkolenia jest nabycie przez uczestników wiedzy oraz umiejętności praktycznych dotyczących ochrony przed atakami cyberprzestępców, wirusami, złośliwym oprogramowaniem, także w zakresie bezpiecznego zarządzania danymi w przedsiębiorstwie, włączając w to wrażliwe dane osobowe, a także zagrożeń płynących z korzystania z Internetu, mediów społecznościowych, poczty e-mail.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
WIEDZA: -Uczestnik zna zasady bezpiecznego korzystania z Internetu, poczty e-mail oraz mediów społecznościowych i chmury, używa odpowiednich narzędzi do ochrony przed atakami cyberprzestępców oraz przed złośliwym oprogramowaniem, potrafi rozpoznać zagrożenie płynące z sieci i skutecznie je zneutralizować, zna zasady funkcjonowania metod socjotechnicznych w celu wyłudzenia danych (m.in. phishing)	Efekty uczenia się zostaną zweryfikowane na podstawie warsztatów oraz praktycznych unikalnych metod.	Prezentacja
UMIEJĘTNOŚCI: -Uczestnik potrafi obsługiwać przeglądarkę w trybie prywatnym umie "zacierać za sobą ślady" pozostawione w Internecie tworzy i korzysta z kopii bezpieczeństwa zna ryzyko wykradnięcia danych i umie je zminimalizować potrafi reagować po wykryciu u siebie w firmie incydentu naruszenia bezpieczeństwa wie jak postępować w przypadku wykrycia w swoim sprzęcie komputerowym złośliwego oprogramowania	Efekty uczenia się zostaną zweryfikowane na podstawie warsztatów oraz praktycznych unikalnych metod.	Obserwacja w warunkach rzeczywistych
KOMPETENCJE: -Uczestnik potrafi rozpoznać fałszywy adres e-mail, aplikację, link, wiadomość na Facebooku ,zna metody wyłudzania danych i umie je zidentyfikować i opisać samodzielnie, rozumie znaczenie komunikacji interpersonalnej ,ma świadomość samokształcenia wie jak zarządzać, przetwarzać, szyfrować dane osobowe, zna sprzętowe możliwości ochrony danych (w tym osobowych) rozumie pojęcia typowe dla zagadnień związanych z cyberbezpieczeństwem (VPN, trojan, malware, i inne)	Efekty uczenia się zostaną zweryfikowane na podstawie warsztatów oraz praktycznych unikalnych metod.	Prezentacja

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.

- Jak dbać o swoją tożsamość cyfrową.

- Wirusy, szpiegowanie, rodzaje, sposoby hackowania systemu operacyjnego.

- Tryb bezpieczny – incognito, monitorowanie zachowań w sieci

- Programy antywirusowe i ochrona przed atakami hakerskimi

- Cookies, monitorowanie IP, MAC, VPN, Historia

- Rodzaje oraz narzędzia wykorzystywane do ataków hakerskich - Phishing, cracking, spoofing, back door, trojan, Dos, keyloggin, session hijacking i inne.

2.

- Zarządzanie i ochrona danych w przedsiębiorstwie

- Szyfrowanie danych

- Kopie bezpieczeństwa

- Ochrona danych osobowych klientów

- Po ataku - studium przypadków

- Incydenty bezpieczeństwa

Harmonogram

Liczba przedmiotów/zajęć: 14

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 14 Jak dbać o swoją tożsamość cyfrową. Wirusy, szpiegowanie, rodzaje, sposoby hakowania. Tryb bezpieczny, monitorowanie zachowań w sieci. Rodzaje oraz narzędzia wykorzystywane do ataków hakerskich.	-	24-07-2024	09:00	10:30	01:30
2 z 14 przerwa	-	24-07-2024	10:30	10:45	00:15
3 z 14 Jak dbać o swoją tożsamość cyfrową. Wirusy, szpiegowanie, rodzaje, sposoby hakowania. Tryb bezpieczny, monitorowanie zachowań w sieci. Rodzaje oraz narzędzia wykorzystywane do ataków hakerskich.	-	24-07-2024	10:45	12:15	01:30
4 z 14 przerwa	-	24-07-2024	12:15	12:30	00:15
5 z 14 Jak dbać o swoją tożsamość cyfrową. Wirusy, szpiegowanie, rodzaje, sposoby hakowania. Tryb bezpieczny, monitorowanie zachowań w sieci. Rodzaje oraz narzędzia wykorzystywane do ataków hakerskich.	-	24-07-2024	12:30	14:00	01:30
6 z 14 przerwa	-	24-07-2024	14:00	14:15	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
7 z 14 Jak dbać o swoją tożsamość cyfrową. Wirusy, szpiegowanie, rodzaje, sposoby hakowania. Tryb bezpieczny, monitorowanie zachowań w sieci. Rodzaje oraz narzędzia wykorzystywane do ataków hakerskich.	-	24-07-2024	14:15	15:45	01:30
8 z 14 Zarządzanie i ochrona danych w przedsiębiorstwie- szyfrowanie danych - kopie bezpieczeństwa - ochrona danych osobowych klientów - po ataku - studium przypadków - incydenty bezpieczeństwa	-	25-07-2024	09:00	10:30	01:30
9 z 14 przerwa	-	25-07-2024	10:30	10:45	00:15
10 z 14 Zarządzanie i ochrona danych w przedsiębiorstwie- szyfrowanie danych - kopie bezpieczeństwa - ochrona danych osobowych klientów - po ataku - studium przypadków - incydenty bezpieczeństwa	-	25-07-2024	10:45	12:15	01:30
11 z 14 przerwa	-	25-07-2024	12:15	12:30	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
12 z 14 Zarządzanie i ochrona danych w przedsiębiorstwie- szyfrowanie danych - kopie bezpieczeństwa - ochrona danych osobowych klientów - po ataku - studium przypadków - incydenty bezpieczeństwa	-	25-07-2024	12:30	14:00	01:30
13 z 14 przerwa	-	25-07-2024	14:00	14:15	00:15
14 z 14 Zarządzanie i ochrona danych w przedsiębiorstwie- szyfrowanie danych - kopie bezpieczeństwa - ochrona danych osobowych klientów - po ataku - studium przypadków - incydenty bezpieczeństwa	-	25-07-2024	14:15	15:45	01:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt usługi brutto	2 730,00 PLN
Koszt usługi netto	2 730,00 PLN
Koszt godziny brutto	170,63 PLN
Koszt godziny netto	170,63 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

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

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 godzina= 45 minut (godzina szkoleniowa)

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

2. E-materiały w formacie PDF.

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

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.

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.

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 Jońca

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