Możliwość dofinansowania

Future Consulting
Monika Ornal-Olech

★★★★★

Bezpieczeństwo w sieci- aplikacje internetowe

Numer usługi 2024/09/09/150920/2299856

4 800,00 PLN brutto
4 800,00 PLN netto
200,00 PLN brutto/h
200,00 PLN netto/h

zdalna w czasie rzeczywistym
Usługa szkoleniowa
24 h
14.10.2024 do 16.10.2024

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikator projektu	Kierunek - Rozwój
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Szkolenie skierowane jest do osób indywidualnych jak i pracujących w branży IT, chcących powiększyć swoją wiedzę na temat bezpiecznego poruszania się w aplikacjach internetowych. Usługa adresowana również do uczestników projektu „Kierunek – Rozwój”.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	8
Data zakończenia rekrutacji	10-10-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	24
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

Szkolenie przygotowuje uczestników do bezpiecznego korzystania z Internetu i bezpiecznego wykorzystywania aplikacji internetowych, w celu poprawienia efektywności swojej pracy.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Prawidłowo ocenia własne zabezpieczenia internetowe.	Uczestnik tworzy bezpieczne hasło do stron internetowych i aplikacji. Poprawnie odpowiada na pytania z teorii i wykonuje zadania praktyczne.	Test teoretyczny Obserwacja w warunkach symulowanych
Samodzielnie broni się przed cyberatakami i rozpoznaje oszustwa w sieci.	Kursant potrafi poprawnie rozróżniać zagrożone sieci, jest w stanie odzyskać utracone dane dzięki aktualizacji oprogramowania.	Test teoretyczny Obserwacja w warunkach rzeczywistych
Wykorzystuje techniki i sposoby walki z hakerami.	Uczestnik obsługuje programy antyspamowe i antywirusowe oraz tworzy zapory sieciowe.	Test teoretyczny 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, dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się.

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

Tak, dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji.

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

Tak, dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji.

Program

->Szkolenie jest adresowane do osób indywidualnych jak i pracujących w branży IT, chcących powiększyć swoją wiedzę na temat bezpiecznego poruszania się w aplikacjach internetowych.

-> W celu skutecznego uczestnictwa, szkolenie adresowane jest do osób posiadających minimum podstawową umiejętność obsługi komputera.

-> Za 1 godzinę usługi szkoleniowej uznaje się godzinę dydaktyczną tj. lekcyjną (45 minut).

-> Ilość przerw oraz długość ich trwania zostanie dostosowana indywidualnie do potrzeb uczestników szkolenia. Zaznacza się jednak, że łączna długość przerw podczas szkolenia nie będzie dłuższa aniżeli zawarta w harmonogramie.

->Przerwy nie wliczają się w czas trwania usługi.

Warunki organizacyjne:

->Skompletowanie jednej grupy uczestników 2-8 osobowej

Moduł 1:

•Wprowadzenie do cyberbezpieczeństwa

• Co to jest cyberbezpieczeństwo?

• Dlaczego cyberbezpieczeństwo jest ważne?

• Rodzaje zagrożeń cybernetycznych

• Wpływ cyberataków na osoby i firmy

• Podstawowe zasady bezpieczeństwa

• Tworzenie silnych haseł

• Ochrona danych osobowych

• Bezpieczne korzystanie z Internetu

• Aktualizowanie oprogramowania

Moduł 2:

• Zagrożenia cybernetyczne

• Malware

• Phishing

• Ransomware

• Ataki sieciowe

• Inżynieria społeczna

• Ochrona przed cyberatakami

• Oprogramowanie antywirusowe i antyspamowe

• Zapory sieciowe

• Szyfrowanie

• Kopie zapasowe

Moduł 3:

• Zarządzanie incydentami bezpieczeństwa

• Identyfikacja incydentów bezpieczeństwa

• Reagowanie na incydenty bezpieczeństwa

• Odzyskiwanie po incydentach bezpieczeństwa

• Zapobieganie przyszłym incydentom bezpieczeństwa

Egzamin przeprowadzany w formie test teoretycznego oraz zadania praktycznego.

Harmonogram

Liczba przedmiotów/zajęć: 18

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 18 •Wprowadzenie do cyberbezpieczeństwa • Co to jest cyberbezpieczeństwo?	MAŁGORZATA BĘDKOWSKA	14-10-2024	09:00	09:45	00:45
2 z 18 • Dlaczego cyberbezpieczeństwo jest ważne? • Rodzaje zagrożeń cybernetycznych	MAŁGORZATA BĘDKOWSKA	14-10-2024	09:45	11:15	01:30
3 z 18 Przerwa	MAŁGORZATA BĘDKOWSKA	14-10-2024	11:15	11:30	00:15
4 z 18 • Wpływ cyberataków na osoby i firmy • Podstawowe zasady bezpieczeństwa	MAŁGORZATA BĘDKOWSKA	14-10-2024	11:30	13:00	01:30
5 z 18 • Tworzenie silnych haseł • Ochrona danych osobowych	MAŁGORZATA BĘDKOWSKA	14-10-2024	13:00	14:30	01:30
6 z 18 • Zagrożenia cybernetyczne • Malware	MAŁGORZATA BĘDKOWSKA	15-10-2024	09:00	09:45	00:45
7 z 18 • Phishing • Ransomware	MAŁGORZATA BĘDKOWSKA	15-10-2024	09:45	11:15	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
8 z 18 Przerwa	MAŁGORZATA BĘDKOWSKA	15-10-2024	11:15	11:30	00:15
9 z 18 • Ataki sieciowe • Inżynieria społeczna	MAŁGORZATA BĘDKOWSKA	15-10-2024	11:30	13:00	01:30
10 z 18 • Ochrona przed cyberatakami • Oprogramowanie antywirusowe i antyspamowe	MAŁGORZATA BĘDKOWSKA	15-10-2024	13:00	14:30	01:30
11 z 18 • Zapory sieciowe • Szyfrowanie • Kopie zapasowe	MAŁGORZATA BĘDKOWSKA	15-10-2024	14:30	15:15	00:45
12 z 18 • Zarządzanie incydentami bezpieczeństwa	MAŁGORZATA BĘDKOWSKA	16-10-2024	09:00	09:45	00:45
13 z 18 • Identyfikacja incydentów bezpieczeństwa	MAŁGORZATA BĘDKOWSKA	16-10-2024	09:45	11:15	01:30
14 z 18 Przerwa	MAŁGORZATA BĘDKOWSKA	16-10-2024	11:15	11:30	00:15
15 z 18 • Reagowanie na incydenty bezpieczeństwa • Odzyskiwanie po incydentach bezpieczeństwa	MAŁGORZATA BĘDKOWSKA	16-10-2024	11:30	13:00	01:30
16 z 18 • Zapobieganie przyszłym incydentom bezpieczeństwa	MAŁGORZATA BĘDKOWSKA	16-10-2024	13:00	14:30	01:30
17 z 18 • Bezpieczne korzystanie z Internetu • Aktualizowanie oprogramowania	MAŁGORZATA BĘDKOWSKA	16-10-2024	14:30	15:15	00:45

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
18 z 18 Egzamin przeprowadzany w formie test teoretycznego oraz zadania praktycznego.	-	16-10-2024	14:30	15:15	00:45

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 800,00 PLN
Koszt przypadający na 1 uczestnika netto	4 800,00 PLN
Koszt osobogodziny brutto	200,00 PLN
Koszt osobogodziny netto	200,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

MAŁGORZATA BĘDKOWSKA

Ukończyła studia wyższe magisterskie na kierunku Pedagogika z edukacją informatyczną oraz podyplomowe na kierunkach: Cyberbezpieczeństwo, Executive MBA - studia menadżerskie. Posiada ponad 15 letnie doświadczenie jako Trenerka oraz szeroki wachlarz tematyk, z w których się specjalizuje m.in. Pracownik biurowy, obsługa programów magazynowych, Cyberbezpieczeństwo oraz sztuczna inteligencja. Jest również czynnym egzaminatorem ECDL, w swojej wieloletniej karierze zdobyła tytuł najlepszego egzaminatora kilkukrotnie. Ukończyła wiele kursów i pozyskała wiele certyfikatów potwierdzających kompetencje. Trenerka posiada wiedzę w zakresie teoretycznych aspektów zagadnień i posiada doświadczenie dydaktyczne oraz praktyczne w dziedzinie, zdobyte w ostatnich 5 latach i wcześniej.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy z uczestników otrzyma materiały dydaktyczne oraz prezentację w formie e-mail.
Trener prowadzący szkolenie na bieżąco będzie przesyłał zadania oraz ćwiczenia.
Po zakończeniu szkolenia każdy z uczestników dostaje zaświadczenie o ukończeniu szkolenia, z zastrzeżeniem obecności nawszystkich zajęciach.

Warunki uczestnictwa

Warunkiem uzyskania zaświadczenia potwierdzającego zdobyte kompetencje jest przystąpienie do egzaminu na zakończenie szkolenia. Na egzamin uczestnik nie musi dokonywać osobnego zapisu.

Koszt egzaminu wliczony jest w cenę usługi i odbędzie się w ustalonym wg harmonogramu szkolenia terminie.

Informacje dodatkowe

Zawarto umowę z WUP w Toruniu w ramach projektu Kierunek – Rozwój.

Kompetencja związana z cyfrową transformacją.

Nie pasuje Ci termin szkolenia? Skontaktuj się z nami!

Telefon: 601 847 454

Mail: kontakt@future-consulting.pl

Warunki techniczne

Wymagania techniczne: Komputer podłączony do Internetu z prędkością łącza od 512 KB/sek.

Minimalne wymagania sprzętowe, jakie musi spełniać komputer Uczestnika lub inne urządzenie do zdalnej komunikacji oraz niezbędneoprogramowanie umożliwiające Uczestnikom dostęp do prezentowanych treści i materiałów

- system operacyjny Windows 7/8/10 lub Mac OS X
- pakiet Microsoft Offi ce, Libre Offi ce, Open Offi ce

Minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnik -

- minimalna prędkość łącza: 512KB/sek

Platforma, na której zostanie przeprowadzone szkolenie to google meet.
Okres ważności linku: **1h** przed rozpoczęciem szkolenia w pierwszym dniu do **ostatniej godziny** w dniu zakończenia.

Kontakt

Monika Ornal-Olech

E-mail monikaornal@wp.pl
Telefon (+48) 601 847 454