Możliwość dofinansowania

Future Consulting
Monika Ornal-Olech

Brak ocen dla tego dostawcy

Bezpieczeństwo w sieci - dla pracownika

Numer usługi 2024/06/24/150920/2194654

1 600,00 PLN brutto
1 600,00 PLN netto
200,00 PLN brutto/h
200,00 PLN netto/h

Lublin / stacjonarna
Usługa szkoleniowa
8 h
18.10.2024 do 18.10.2024

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Szkolenie skierowane jest do osób indywidualnych jak i pracujących w branży IT, chcących powiększyć swoją wiedzę na temat bezpiecznego poruszania się w sieci.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	8
Data zakończenia rekrutacji	17-10-2024
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	8
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 samodzielnej obrony przed cyberatakami i pozwala rozpoznawać oszustwa w sieci. Uczestnik zapoznaje się z podstawowymi problemami zabezpieczeń sieci komputerowych, systemów komputerowych i aplikacji. Celem szkolenia jest także reagowanie na cyber-zagrożenia, poprzez dokonywanie prawidłowej oceny własnych zabezpieczeń oraz wykorzystanie technik i sposobów walki z hakerami.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Prawidłowo ocenia własne zabezpieczenia.	Kursant zna zasady jak stworzyć bezpieczne hasła	Test teoretyczny
		Obserwacja w warunkach symulowanych
Samodzielnie broni się przed cyberatakami i rozpoznaje oszustwa w sieci.	Kursant posiada wiedzę z zakresu ochrony przed cyberatakami i zasad ochrony swoich danych. Bezbłędnie udziela odpowiedzi na zadane pytania.	Test teoretyczny
		Obserwacja w warunkach symulowanych
Wykorzystuje techniki i sposoby walki z hakerami.	Uczestnik obsługuje programy antyspamowe, antywirusowe oraz tworzy zapory sieciowe.	Test teoretyczny 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, 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 sieci.

-> 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

->Przydzielenie każdej z osób indywidualnego stanowiska komputerowego (jedno stanowisko obejmuje: krzesło, biurko, laptop, myszka)

Moduł 1:

•Wprowadzenie do cyberbezpieczeństwa

• Rodzaje zagrożeń cybernetycznych

• Podstawowe zasady bezpieczeństwa

• Tworzenie silnych haseł

• Ochrona danych osobowych

Moduł 2:

• Zagrożenia cybernetyczne

• Ataki sieciowe

• Ochrona przed cyberatakami

• Oprogramowanie antywirusowe i antyspamowe

• Zapory sieciowe

• Szyfrowanie

• Kopie zapasowe

Moduł 3:

• Zarządzanie incydentami bezpieczeństwa

• Identyfikacja incydentów bezpieczeństwa

• Reagowanie na incydenty bezpieczeństwa

• Zapobieganie przyszłym incydentom bezpieczeństwa

Egzamin przeprowadzany w formie test teoretycznego oraz zadania praktycznego.

Harmonogram

Liczba przedmiotów/zajęć: 6

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 6 Wprowadzenie do cyberbezpieczeństwa	Adrian Flak	18-10-2024	09:00	09:45	00:45
2 z 6 • Rodzaje zagrożeń cybernetycznych • Podstawowe zasady bezpieczeństwa • Tworzenie silnych haseł • Ochrona danych osobowych	Adrian Flak	18-10-2024	09:45	11:15	01:30
3 z 6 Przerwa	Adrian Flak	18-10-2024	11:15	11:30	00:15
4 z 6 • Zagrożenia cybernetyczne • Ataki sieciowe • Ochrona przed cyberatakami • Oprogramowanie antywirusowe i antyspamowe • Zapory sieciowe • Szyfrowanie • Kopie zapasowe	Adrian Flak	18-10-2024	11:30	13:00	01:30
5 z 6 • Zarządzanie incydentami bezpieczeństwa • Identyfikacja incydentów bezpieczeństwa • Reagowanie na incydenty bezpieczeństwa • Zapobieganie przyszłym incydentom bezpieczeństwa	Adrian Flak	18-10-2024	13:00	14:30	01:30
6 z 6 Egzamin przeprowadzany w formie test teoretycznego oraz zadania praktycznego.	-	18-10-2024	14:30	15:15	00:45

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 600,00 PLN
Koszt przypadający na 1 uczestnika netto	1 600,00 PLN
Koszt osobogodziny brutto	200,00 PLN
Koszt osobogodziny netto	200,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Adrian Flak

Ukończył studia wyższe I i II stopnia na kierunku Informatyka. Praktyk i szkoleniowiec z zakresu IT, głównie E-commerce, SEO, SEM oraz programowania. Przeprowadził wiele szkoleń dotyczących nowoczesnych technik sprzedażowych w Internecie oraz programowania. Ukończył kursy ORACLE związane z JEE7 czy SQL. Zrealizował wiele projektów E-commerce oraz pracował na stanowiskach związanych z tą branżą. Trener posiada wiedzę w zakresie teoretycznych aspektów zagadnień i posiada doświadczenie dydaktyczne oraz praktyczne w dziedzinie.

Trener posiada odpowiednie do rodzaju i zakresu świadczonych usług doświadczenie zawodowe, nabyte w ciągu ostatnich 5 lat od daty publikacji usługi.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy z uczestników otrzyma tematyczne materiały dydaktyczne w postaci skryptów oraz prezentacji w formie pdf, przesłanych na adrese-mail, najpóźniej w dniu rozpoczęcia szkolenia.

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

Nie pasuje Ci termin szkolenia? Skontaktuj się z nami!

Telefon: 601 847 454

Mail: kontakt@future-consulting.pl

Adres

ul. Agatowa 5/U9D
20-400 Lublin
woj. lubelskie

Szkolenie odbędzie się w sali szkoleniowej zlokalizowanej przy ul. Agatowej 5/U9D w Lublinie.

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi

Kontakt

Monika Ornal-Olech

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