Możliwość dofinansowania

ADN AKADEMIA spółka z ograniczoną odpowiedzialnością spółka komandytowa

★★★★½

Cyberbezpieczeństwo. Zbiór praktyk i technologii mających na celu ochronę systemów komputerowych, sieci i danych przed nieuprawnionym dostępem, atakami i szkodami. Ochronę poufności, integralności i dostępności informacji w środowisku cybernetycznym.

Numer usługi 2024/09/09/47095/2299593

zdalna w czasie rzeczywistym
Usługa szkoleniowa
8 h
29.11.2024 do 29.11.2024

1 280,00 PLN brutto
1 280,00 PLN netto
160,00 PLN brutto/h
160,00 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla pracodawców i ich pracowników wsparcie dla osób indywidualnych
Grupa docelowa usługi	Szkolenie skierowane jest do osób indywidualnych jak i pracujących wbranży IT,chcących powiększyć swoja wiedzę na temat bezpiecznegoporuszania się w sieci. Jest to usługa dedykowana, również dla uczestników projektu „Kierunek- Rozwój"
Minimalna liczba uczestników	10
Maksymalna liczba uczestników	25
Data zakończenia rekrutacji	25-11-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	8
Podstawa uzyskania wpisu do BUR	Certyfikat VCC Akademia Edukacyjna

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 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
Prawidło ocenia własne zabezpieczenia	- Tworzy bezpieczne hasło - Stosuje umiejętność oceny siły własnego hasła	Test teoretyczny
		Obserwacja w warunkach symulowanych
	-Definiuje rodzaje zagrożeń cybernetycznych	Test teoretyczny
		Obserwacja w warunkach symulowanych
Samodzielnie zarządza obroną przed cyberatakami i rozpoznaje oszustwa w sieci.	- Odzyskuje utracone dane	Test teoretyczny
		Obserwacja w warunkach symulowanych
	- Aktualizuje oprogramowanie	Test teoretyczny
		Obserwacja w warunkach symulowanych
Wykorzystuje techniki i sposoby walki z hakerami.	-Obsługuje programy antyspamowe i antywirusowe	Test teoretyczny
		Obserwacja w warunkach symulowanych
	-Stosuje 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

W celu skutecznego uczestnictwa w szkoleniu wymagana jest podstawowa umiejętność obsługi komputera.

Szkolenie przeprowadzone będzie w formie zdalnej w czasie rzeczywistym w liczbie 8 godzin, z wykorzystaniem kamery i mikrofonu. Każdy uczestnik musi posiadać dostęp do komputera z internetem. Uczestnikom zostanie przesłany link do videokonferencji na platformie google meet.

Podczas szkolenia zapewnione są przerwy - harmonogram szkolenia.

Moduł 1:

- Wprowadzenie do cyberbezpieczeństwa
- Co to jest cyberbezpieczeństwo?
- Dlaczego cyberbezpieczeństwo jest ważne?
- Rodzaje zagrożeń cybernetycznych
- Wpływ cyberataków na osoby i fi rmy
- Aktualizowanie oprogramowania
- Podstawowe zasady bezpieczeństwa
- Tworzenie silnych haseł
- Ochrona danych osobowych
- Bezpieczne korzystanie z Internetu
- Aktualizowanie oprogramowania

Moduł 2:

- 1. Zagrożenia cybernetyczne
- Malware
- Phishing
- Ransomware
- Ataki sieciowe
- Inżynieria społeczna
- Ochrona przed cyberatakami
- Oprogramowanie antywirusowe i antyspamowe
- Zapory sieciowe
- Szyfrowanie
- Kopie zapasowe

Moduł 3.

- 1. Zarządzanie incydentami bezpieczeństwa
- Identyfi kacja incydentów bezpieczeństwa
- Reagowanie na incydenty bezpieczeństwa
- Odzyskiwanie po incydentach bezpieczeństwa
- Zapobieganie przyszłym incydentom bezpieczeństwa

Test teoretyczny.

Harmonogram

Liczba przedmiotów/zajęć: 8

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 8 MODUŁ I	Łukasz Kwiecień	29-11-2024	08:00	10:00	02:00
2 z 8 Przerwa	Łukasz Kwiecień	29-11-2024	10:00	10:10	00:10
3 z 8 C.D. MODUŁ I	Łukasz Kwiecień	29-11-2024	10:10	12:00	01:50
4 z 8 Przerwa	Łukasz Kwiecień	29-11-2024	12:00	12:10	00:10
5 z 8 MODUŁ II	Łukasz Kwiecień	29-11-2024	12:10	14:00	01:50
6 z 8 Przerwa	Łukasz Kwiecień	29-11-2024	14:00	14:10	00:10
7 z 8 MODUŁ III	Łukasz Kwiecień	29-11-2024	14:10	15:30	01:20
8 z 8 TEST TEORETYCZNY	-	29-11-2024	15:30	16:00	00:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 280,00 PLN
Koszt przypadający na 1 uczestnika netto	1 280,00 PLN
Koszt osobogodziny brutto	160,00 PLN
Koszt osobogodziny netto	160,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Łukasz Kwiecień

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.

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 certyfi katu potwierdzającego zdobyte kompetencje jest przystąpienie do testu sprawdzającego. Na egzami nuczestnik nie musi dokonywać osobnego zapisu.

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

Nazwa podmiotu prowadzącego walidację: ERNABO Adrian Flak

Zostaną zastosowane rozwiązania zapewniające rozdzielenie procesów kształcenia i szkolenia od walidacji.

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 orazniezbędneoprogramowanie 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
- uczestnik musi posiadać dostęp do kamery i mikrofonu- wymóg konieczny

Minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnik
-mminimalna prędkość łącza:512KB/sek

Szkolenie zostanie przeprowadzone na platformie szkoleniowej.

Okres ważności linku: 1h przed rozpoczęciem szkolenia w pierwszym dniu do ostatniej godziny w dniu zakończenia.

Podstawą do rozliczenia usługi jest wygenerowanie z systemu raportu, umożliwiającego identyfi kację wszystkich uczestników i zastosowanego narzędzia.

Szkolenia online będą nagrywane tylko i wyłącznie na potrzeb udokumentowania prawidłowego przebiegu szkolenia i jego archiwizacji.Nie udostępniamy nagrań ze szkolenia ze względu na ochronę danych osobowych oraz widocznego na nagraniach wizerunku osóbtrzecich (osoby prowadzącej oraz innych uczestników szkolenia).

Kontakt

Ariel Banaszewski

E-mail ariel.banaszewski@adn.pl

Telefon (+48) 22 1627 981