Możliwość dofinansowania

Cyberbezpieczeństwo - o realnych i bieżących zagrożeniach w organizacji

Numer usługi 2024/06/07/5241/2175488

1 560,00 PLN brutto
1 560,00 PLN netto
195,00 PLN brutto/h
195,00 PLN netto/h

OŚRODEK SZKOLENIOWO-WDROŻENIOWY MAREK SZARATA SP. Z O. O.

★★★★★

Bydgoszcz / stacjonarna
Usługa szkoleniowa
8 h
06.09.2024 do 06.09.2024

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Przedsiębiorcy i pracownicy, którzy chcą pozyskać rozwiązania i propozycje w zakresie zapewnienia bezpieczeństwa danych osobowych oraz informacji poufnych.
Minimalna liczba uczestników	12
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	05-09-2024
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	8
Podstawa uzyskania wpisu do BUR	Certyfikat ICVC - SURE (Standard Usług Rozwojowych w Edukacji): Norma zarządzania jakością w zakresie świadczenia usług rozwojowych

Cel

Cel edukacyjny

Przygotowuje do samodzielnej pracy przy wykorzystaniu najlepszych praktyk bezpieczeństwa danych, skutecznego reagowania na incydenty cyberbezpieczeństwa i promocji kultury bezpieczeństwa w firmie poprzez aktywne

zaangażowanie innych pracowników w ochronę danych i świadomość zagrożeń.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik stosuje najlepsze praktyki bezpieczeństwa danych i skutecznie reaguje na incydenty cyberbezpieczeństwa.	Definiuje kluczowe terminy i pojęcia związane z cyberbezpieczeństwem	Test teoretyczny
	Ocenia ryzyko związane z cyberatakami, identyfikuje słabe punkty w systemach i procedurach bezpieczeństwa	Test teoretyczny
	Stosuje prawidłowe techniki zapobiegania atakom.	Test teoretyczny
	Prawidłowo reaguje na incydenty związane z atakami.	Test teoretyczny
Uczestnik promuje kulturę bezpieczeństwa w firmie poprzez aktywne zaangażowanie innych pracowników w ochronę danych i świadomość zagrożeń.	Efektywnie współpracuje z innymi pracownikami w zakresie zapewniania bezpieczeństwa danych.	Test teoretyczny
	Promuje kulturę bezpieczeństwa cyfrowego w organizacji.	Test teoretyczny
	Prawidłowo komunikuje się z zespołem w celu identyfikacji i rozwiązywania problemów związanych z bezpieczeństwem informatycznym.	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

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?

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?

Dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji.

Program

Usługa szkoleniowa skierowana jest do przedsiębiorców i pracowników, którzy chcą pozyskać rozwiązania i propozycje w zakresie zapewnienia bezpieczeństwa danych osobowych oraz informacji poufnych.

8:30 – 11:45 (1 przerwa 15 minut)

Blok teoretyczny:

1. Rodzaje ataków - przyczyny, źródła, cel i mechanizmy ataków
2. Czym jest socjotechnika i jak się przed nią bronić?
3. Rozpoznawanie złośliwego oprogramowania, phishingu, fałszywych informacji
4. Jak bezpiecznie komunikować się w Internecie?
5. Użytkowanie menadżera haseł, szyfrowanie danych
6. Prawidłowe korzystanie z komputera - w jaki sposób zabezpieczyć własne dane?
7. Przykłady incydentów bezpieczeństwa informacji - największe wycieki danych z ostatnich lat
8. DYSKUSJA. Pytania i odpowiedzi

12:15 – 15:00 (1 przerwa 15 minut)

Blok praktyczny:

1. Rozpoznawanie przykładowych wiadomości phishingowych, złośliwego oprogramowania – interaktywne testy
2. Ćwiczenia z obsługi menadżera haseł, szyfrowania danych

15:00 – 15:30

Walidacja

Szkolenie odbywać się będzie bez podziału na grupy. Zajęcia praktyczne realizowane będą przy komputerach – 1 stanowisko na uczestnika.

Czas szkolenia został podany w godzinach dydaktycznych, czyli 1 godzina szkolenia równa się 45 minut. W ciągu dnia zaplanowane zostały 3 przerwy (2 przerwy po 15 minut i jedna – 30 minut), które nie zostały wliczone w czas trwania usługi.

Harmonogram

Liczba przedmiotów/zajęć: 8

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 8 Blok teoretyczny	Adrian Iwanek	06-09-2024	08:30	10:00	01:30
2 z 8 Przerwa	Adrian Iwanek	06-09-2024	10:00	10:15	00:15
3 z 8 Blok teoretyczny	Adrian Iwanek	06-09-2024	10:15	11:45	01:30
4 z 8 Przerwa	Adrian Iwanek	06-09-2024	11:45	12:15	00:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 8 Blok praktyczny	Adrian Iwanek	06-09-2024	12:15	13:45	01:30
6 z 8 Przerwa	Adrian Iwanek	06-09-2024	13:45	14:00	00:15
7 z 8 Blok praktyczny	Adrian Iwanek	06-09-2024	14:00	15:00	01:00
8 z 8 Walidacja	-	06-09-2024	15:00	15:30	00:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 560,00 PLN
Koszt przypadający na 1 uczestnika netto	1 560,00 PLN
Koszt osobogodziny brutto	195,00 PLN
Koszt osobogodziny netto	195,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Adrian Iwanek

Adrian Iwanek to doświadczony ekspert posiadający rozległą wiedzę zarówno w dziedzinie cyberbezpieczeństwa, jak i w praktycznym wykorzystaniu technologii zabezpieczeń. Jako specjalista z wieloletnim doświadczeniem w dziedzinie programowania i cyberbezpieczeństwa, ma głęboką znajomość wszystkich aspektów bezpieczeństwa informatycznego oraz doskonałą umiejętność praktycznego stosowania narzędzi cyberbezpieczeństwa. Jego zaangażowanie w rozwój technologii zabezpieczeń oraz umiejętność przekazywania wiedzy sprawiają, że jest idealnym wyborem na trenera dla tego rodzaju szkoleń.
Wykształcenie:
- Wyższa Szkoła Informatyki - Inżynieria Oprogramowania - 2009
Szkolenia:
- Dlaczego hackowanie aplikacji webowych jest proste? – 11.2022
- Wprowadzenie do bezpieczeństwa IT – 03.2023
- Dlaczego hackowanie aplikacji webowych jest proste? Edycja 2024 r. – 01.2024

- Wprowadzenie do bezpieczeństwa Linux - 02.2024
- Analiza po włamaniowa w Linuksie – 02.2024
- Praktyczny rekonesans infrastruktury IT – 04.2024

Doświadczenie trenerskie:
- Gmina Wierzchowo. Praktyczne szkolenie z cyberbezpieczeństwa – 03.2023
- Powiat Iławski - 7 bloków szkoleniowych dla ponad 100 osób dla starostwa i jednostek podległych – 04.2023
- Audyty infrastruktury dla 6 szpitali - 10-11.2023
- Webinary i wystąpienia na konferencjach poświęconych cyberbezpieczeństwu – 2022-2024.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały merytoryczne, związane z tematyką szkolenia w postaci skryptu dla każdego z uczestników.

Warunki uczestnictwa

Szczegółowe warunki udziału w szkoleniu określa Regulamin szkoleń, w tym zgodę uczestnika na użyczenie swojego wizerunku w charakterze zdjęć, filmów zrobionych podczas szkolenia, w którym uczestniczył.

Adres

ul. Maksymiliana Piotrowskiego 11
85-098 Bydgoszcz
woj. kujawsko-pomorskie

Udogodnienia w miejscu realizacji usługi

- Laboratorium komputerowe
- Klimatyzacja
- Wi-fi

Kontakt

Piotr Szarata

E-mail osw@osw.bydgoszcz.pl
Telefon (+48) 509 705 517