Możliwość dofinansowania

Wektor Wiedzy Sp. z o.o.

★★★★½

Bezpieczeństwo informacji – aktualne zagrożenia cyberprzestępczością

Numer usługi 2024/04/29/43371/2137898

Jaroszowice / stacjonarna
Usługa szkoleniowa
12 h
26.09.2024 do 27.09.2024

2 788,41 PLN brutto
2 267,00 PLN netto
232,37 PLN brutto/h
188,92 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Osoby zainteresowane zagadnieniami bezpieczeństwa i zasad poruszania się po wirtualnej rzeczywistości. Samodzielni księgowi, główni księgowi, dyrektorzy finansowi oraz pracownicy działów finansowych i księgowości, prowadzący i pracownicy biur rachunkowych a także inni uzytkownicy cyberprzestrzeni - także w ramach zadań zawodowych. Szkolenie jest przydatne każdej osobie, która na co dzień w swojej pracy korzysta z komputera oraz innych urządzeń z dostępem do Internetu.
Minimalna liczba uczestników	10
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	19-09-2024
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	12
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

Kurs przygotowuje do samodzielnej pracy w wirtualnej rzeczywistości, ze świadomością zagrożeń związanych z cyberprzestępczością oraz znajomością metod identyfikacji zagrożeń i reagowania na nie.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wiedza: Uczestnik definiuje pojęcie cyberprzestępczość oraz najpowszechniejsze rodzaje ataków i zagrożeń. Charakteryzuje dobre praktyki związane z bezpiecznym wykorzystaniem firmowych zasobów. Określa jakie zasady pracy zdalnej pomogą mu skutecznie zabezpieczyć się przed 99% ataków.		
Umiejętności: Uczestnik monitoruje incydenty bezpieczeństwa teleinformatycznego. Korzysta z zabezpieczeń w codziennej pracy, unika aplikacji i programów, których należy się wystrzegać. Używa bezpieczne hasła oraz organizery haseł.	Uczestnik przystąpi do testu, który sprawdzi czy osiągnął założone efekty usługi.	Test teoretyczny
Kompetencje społeczne: Pracuje ze świadomością poziomu swojej wiedzy i umiejętności, definiuje swoje potrzeby w zakresie samokształcenia, prawidłowo identyfikuje i rozstrzyga dylematy związane z wykonywaniem zawodu.		

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

Tak, zawiera informacje dotyczące pozyskanej wiedzy, umiejętności i kompetencji społecznych.

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

Tak, zawiera potwierdzenie.

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

Tak, zawiera potwierdzenie.

Program

1. Podstawy bezpieczeństwa teleinformatycznego

Co to jest cyberbezpieczeństwo - definicja cyberprzestrzeni i cyberbezpieczeństwa, dlaczego to jest ważne?

- Aktualność problemu bezpieczeństwa teleinformatycznego.
- Ryzyko i zarządzanie ryzykiem - co to jest ryzyko, podstawowe pojęcia i zasady zarządzania
- ryzykiem.
- Polityka bezpieczeństwa - czym jest w organizacji polityka bezpieczeństwa i jaka jest jej rola?
- Incydenty bezpieczeństwa - co należy rozumieć jako incydent bezpieczeństwa i jak z nim
- postępować?
- Normy i standardy bezpieczeństwa - powszechnie stosowane rozwiązania, norma ISO27001.

2. Ataki „na człowieka" tzw. SOCJOTECHNIKA (stosowane techniki manipulacji)

- Ataki socjotechniczne - techniki manipulacji wykorzystywane przez cyberprzestępców.
- Sposoby - pod jakimi pretekstami wyłudza się firmowe dokumenty.
- Wykrywanie - jak rozpoznać, że jest się celem ataku socjotechnicznego.
- Reakcja - jak prawidłowo reagować na ataki socjotechniczne.
- Jak i skąd atakujący zbierają dane na twój temat.
- Miejsca, w których zostawiamy swoje dane świadomie i nieświadomie - jak świadomie udostępniać
- informacje w sieci.

3. Monitorowanie incydentów bezpieczeństwa teleinformatycznego

- Diagnozowanie incydentów.
- Zbieranie danych dotyczących incydentów.
- Analiza danych dotyczących incydentów.
- Podejmowanie działań naprawczych.
- Mechanizmy ochrony przed zagrożeniami bezpieczeństwa sieci teleinformatycznej
- Narzędzia i aplikacje do zabezpieczania sieci.
- Systemy wykrywania włamań i ataków.
- Zapory sieciowe.
- Bezpieczna konfiguracja narzędzi do zarządzania i monitorowania urządzeń
- sieciowych.

4. Metody i środki ochrony informacji

- Bezpieczeństwo fizyczne.
- Bezpieczeństwo programowe.
- Podstawowe zasady ochrony komputerów i telefonów służbowych.
- Kopie zapasowe.
- Polityka stosowania rozwiązań kryptograficznych i szyfrowanie informacji
- przedsięwzięcia organizacyjne.
- Zarządzanie uprawnieniami użytkowników systemów informatycznych, kontrola dostępu.

5. Atak „na komputery" - demonstracje wraz z objaśnieniem metod ochrony

- Przegląd aktualnych ataków komputerowych wykorzystywanych przez cyberprzestępców, typowe
- błędy zabezpieczeń wykorzystywane przez atakujących.
- Ataki przez sieci bezprzewodowe (WiFi, Bluetooth, NFC).
- Ataki przez pocztę e-mail (fałszywe e-maile).
- Ataki przez strony WWW - jak nie dać się zainfekować, fałszywe strony.
- Ataki przez komunikatory (Skype, Facebook).
- Ataki przez telefon (fałszywe SMS-y, przekierowania rozmów, itp.).
- Ataki APT, phishing, smishing, spear-phishing, pharming, spoofing, spam, spim

6. Cyberprzestępczość - najpowszechniejsze rodzaje ataków i zagrożeń – praktyczne case study przypadków

- phishing i inne odmiany ataków socjotechnicznych
- pozostałe zagrożenia dla bezpieczeństwa sieci teleinformatycznej:
- cracking
- sniffing
- metoda salami

- fałszywe powiadomienia z mediów społecznościowych
- oszustwo na „nigeryjskiego księcia”
- skimming

7. Organizacja bezpiecznej sieci teleinformatycznej i bezpieczeństwa informacji – rozwiązania systemowe i wymagania prawne w Polsce

- Norma ISO 27001:2017.

Rozporządzenie o Ochronie Danych Osobowych oraz norma ISO 27701.

Harmonogram

Liczba przedmiotów/zajęć: 2

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 2 BEZPIECZEŃSTWO INFORMACJI – AKTUALNE ZAGROŻENIA CYBERPRZESTĘPCZOŚCIĄ - dzień 1	Michał Dydycz	26-09-2024	09:00	15:00	06:00
2 z 2 BEZPIECZEŃSTWO INFORMACJI – AKTUALNE ZAGROŻENIA CYBERPRZESTĘPCZOŚCIĄ - dzień 2	Michał Dydycz	27-09-2024	09:00	15:00	06:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 788,41 PLN
Koszt przypadający na 1 uczestnika netto	2 267,00 PLN
Koszt osobogodziny brutto	232,37 PLN
Koszt osobogodziny netto	188,92 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Michał Dydycz

Certyfikowany audytor wiodący normy 27001 (bezpieczeństwo informacji), ekspert z cyberbezpieczeństwa i ochrony danych osobowych oraz wdrożeniowiec systemów bezpieczeństwa informacji. Inspektor ds. poświadczenia tożsamości cyfrowej. Prowadził szkolenia zarówno dla jednostek samorządów terytorialnych jak i dla firm prywatnych.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnik usługi otrzyma komplet materiałów szkoleniowych przygotowany przez prowadzących:

- Skrypt

- Prezentacja

Warunki uczestnictwa

Umiejętność pracy z komputerem, znajomość środowiska Windows, Internet

Informacje dodatkowe

Cena bez VAT dla opłacających szkolenie, w co najmniej 70% ze środków publicznych.

Zapraszamy do odwiedzenia naszej strony internetowej: https://wektorwiedzy.pl/

Adres

ul. Zakopiańska 64
34-100 Jaroszowice
woj. małopolskie

Młyn Jacka Hotel & SPA

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Udogodnienia dla osób ze szczególnymi potrzebami

Kontakt

Anna Wilk

E-mail a.wilk@wektorwiedzy.pl

Telefon (+48) 17 2831 004