Możliwość dofinansowania

edpo.pl Michał Cupiał

Brak ocen dla tego dostawcy

Warsztaty świadomości cyberzagrożeń oraz reakcji na incydenty bezpieczeństwa w MMŚP

Numer usługi 2024/06/25/160750/2197151

Olsztyn / mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)

Usługa szkoleniowa

11 h

12.08.2024 do 12.08.2024

3 690,00 PLN brutto

3 000,00 PLN netto

335,45 PLN brutto/h

272,73 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 odpowiedzialne za strategiczne decyzje i politykę organizacji, w tym zarządzanie ryzykiem; - eksperci odpowiedzialni za monitorowanie, wykrywanie i reagowanie na zagrożenia cybernetyczne; - osoby odpowiedzialne za zgodność z przepisami, politykę bezpieczeństwa oraz szkolenia pracowników; - osoby, które na co dzień korzystają z systemów informatycznych i mają dostęp do danych wrażliwych; - osoby odpowiedzialne za obsługę biura, przetwarzanie danych pracowników/klientów oraz komunikację z klientami
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	2
Data zakończenia rekrutacji	08-08-2024
Forma prowadzenia usługi	mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)
Liczba godzin usługi	11
Podstawa uzyskania wpisu do BUR	Certyfikat VCC Akademia Edukacyjna

Cel

Cel edukacyjny

Szkolenie zapewnia uczestnikom dogłębną wiedzę teoretyczną i praktyczną, pozwalając na skuteczne rozpoznawanie i reagowanie na różnorodne zagrożenia w codziennym użytkowaniu technologii. Dodatkowo, uczestnicy zyskują wiedzę na temat zarządzania incydentami, tworzenia planów reakcji oraz przeprowadzania audytów bezpieczeństwa, co pozwala na skuteczniejsze przygotowanie organizacji na ewentualne zagrożenia.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik rozróżnia i definiuje rodzaje zagrożeń cybernetycznych, takich jak phishing, malware, ransomware, i ataki socjotechniczne, co umożliwia szybką identyfikację potencjalnych ataków w rzeczywistych sytuacjach.	Uczestnik identyfikuje różne rodzaje zagrożeń cybernetycznych, rozpoznaje charakterystyczne cechy tych zagrożeń.	Test teoretyczny
Uczestnik nadzoruje ochronę danych osobowych oraz informacji firmowych. Kontroluje bezpieczne korzystanie z internetu, zarządza hasłami i zabezpiecza urządzenia przed nieautoryzowanym dostępem.	Uczestnik identyfikuje bezpieczne strony w internecie, rozróżnia potencjalne zagrożenia. Konstruuje silne i unikalne hasła, które są trudne do złamania.	Test teoretyczny
Uczestnik charakteryzuje i reaguje na incydenty bezpieczeństwa. Podejmuje działania w celu zminimalizowania szkód.	Uczestnik ocenia stopień zagrożenia, jakie niesie ze sobą naruszenie. Klasyfikuje incydenty według ich wpływu na bezpieczeństwo danych oraz ciągłość działania organizacji. Dobiera działania w celu zminimalizowania szkód po wykryciu incydentu.	Test teoretyczny

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 (certyfikat) zawiera opis efektów uczenia się w postaci suplementu.

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

1. Wprowadzenie do Cyberbezpieczeństwa. Podstawy Cyberbezpieczeństwa.
2. Typy Cyberzagrożeń i Ochrona przed Nimi.
3. Bezpieczeństwo Sieciowe
4. Przerwa.
5. Ochrona Danych i Prywatność
6. Zarządzanie Incydentami Bezpieczeństwa
7. Praktyczne Ćwiczenia i Podsumowanie
8. Walidacja – test on-line

Harmonogram

Liczba przedmiotów/zajęć: 7

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
1 z 7 Wprowadzenie do Cyberbezpieczeństwa. Podstawy Cyberbezpieczeństwa	Marcin Smoliński	12-08-2024	08:00	09:00	01:00	Tak
2 z 7 Typy cyberzagrożeń i ochrona przed nimi	Marcin Smoliński	12-08-2024	09:00	11:00	02:00	Tak
3 z 7 Bezpieczeństwo Sieciowe	Marcin Smoliński	12-08-2024	11:00	12:00	01:00	Tak
4 z 7 Ochrona Danych i Prywatność	Marcin Smoliński	12-08-2024	12:15	13:45	01:30	Tak
5 z 7 Zarządzanie Incydentami Bezpieczeństwa	Marcin Smoliński	12-08-2024	13:45	15:15	01:30	Tak

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
6 z 7 Praktyczne Ćwiczenia i Podsumowanie	Marcin Smoliński	12-08-2024	15:15	16:00	00:45	Tak
7 z 7 Walidacja - test on line	-	12-08-2024	16:00	16:15	00:15	Nie

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 690,00 PLN
Koszt przypadający na 1 uczestnika netto	3 000,00 PLN
Koszt osobogodziny brutto	335,45 PLN
Koszt osobogodziny netto	272,73 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Marcin Smoliński

Absolwent uczelni wyższych na kierunkach Administracja, Informatyka (zastosowanie technologii informacyjnych), studiów podyplomowych z zakresu ochrony danych oraz administratora danych jak i efektywnej administracji systemami Linuksowymi. Zdobytą wiedzę potwierdzają także liczne certyfikaty międzynarodowe, min. ISTQB Certified Tester, ITIL Foundation v.3, PRINCE2. Jest również Audytorem Wiodący Systemu Zarządzania Bezpieczeństwem Informacji wg normy PN-EN ISO/IEC 27001.
Kierownik kilkunastu projektów w zakresie wdrożenia i uruchomienia systemów dziedzinowych, systemu obiegu dokumentów, systemów informacji przestrzennych w jednostkach samorządu terytorialnego oraz biznesu w tym koordynator dostaw sprzętu i usług szkoleniowych. Współautor oprogramowania dedykowanego Inspektorom Ochrony Danych oraz Sygnalistom. Prowadzi warsztaty z zakresu bezpieczeństwa informacji oraz cyberbezpieczeństwa.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Na materiały składają się:
1. Prezentacja szkoleniowa.
2. Skrypt szkoleniowy.
3. Ewentualne materiały utworzone w trakcie trwania szkolenia.

Informacje dodatkowe

Techniki aktywne podczas zajęć: prezentacja przygotowana przez trenera, dyskusja, praca na dokumentacji przedsiębiorstwa.

Szkolenie odbywa się w godzinach dydaktycznych, czyli 1 godzina szkolenia równa się 45 minut.

Walidacja efektów usługi odbędzie się z wykorzystaniem testu cyfrowego zgodnie z harmonogramem szkolenia.

Szkolenie uwzglednia przerwy, które nie są wliczone do czasu trwania usługi.

Warunki techniczne

Uczestnik musi dysponować:

komputerem stacjonarnym albo laptopem, ewentualnie tabletem spełniającym wymagania sprzętowe określone dla wykorzystania aplikacji Microsoft Teams określone tu: https://learn.microsoft.com/pl-pl/microsoftteams/hardware-requirements-for-the-teams-app,

zainstalowaną przeglądarką internetową Google Chrome, Mozilla FireFox, Safari lub Explorer w najnowszej dostępnej wersji,

indywidualnym kontem poczty elektronicznej e-mail,

łączem internetowym zapewniającym transfer 100 Mb/s lub wyższym, transferem mobilnym 4G, LTE, LTE+, 5G lub szybszym.

Adres

ul. Jagiellońska 59
10-283 Olsztyn
woj. warmińsko-mazurskie

Kontakt

Anna Smolińska

E-mail anna.smolinska@edpo.pl
Telefon (+48) 881 266 777