



BLU PROFESSIONAL
SKILLS INSTITUTE
SPÓŁKA Z
OGRANICZONĄ
ODPOWIEDZIALNOŚĆ
CIĄ

Brak ocen dla tego dostawcy

Cyberbezpieczeństwo dla przedsiębiorstw

Numer usługi 2024/08/21/171618/2272981

📍 Bydgoszcz / stacjonarna

📄 Usługa szkoleniowa

🕒 8 h

📅 16.12.2024 do 16.12.2024

960,00 PLN brutto

780,49 PLN netto

120,00 PLN brutto/h

97,56 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikator projektu	Kierunek - Rozwój
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	<ul style="list-style-type: none">• Menedżerowie IT• Administratorzy systemów• Specjaliści ds. bezpieczeństwa informacji• Pracownicy działów HR i finansów• Osoby odpowiedzialne za zgodność z regulacjami, takimi jak RODO• Pozostali pracownicy mający dostęp do systemu• Usługa adresowana również dla Uczestników Projektu Kierunek – Rozwój
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	09-12-2024
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

Szkolenie „Cyberbezpieczeństwo w przedsiębiorstwach” przygotowuje uczestników do samodzielnego podejmowania działań w zakresie identyfikacji, analizy oraz zarządzania zagrożeniami cybernetycznymi, a także do reagowania na incydenty bezpieczeństwa w zgodzie z obowiązującymi procedurami i najlepszymi praktykami branżowymi. Po zakończeniu szkolenia uczestnik będzie w stanie wdrożyć skuteczne strategie ochrony danych oraz infrastruktury IT w swojej organizacji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozróżnia rodzaje ataków cybernetycznych i wdraża metody ochrony przed nimi.	Identyfikuje typowe ataki, takie jak phishing, ransomware i DDoS.	Test teoretyczny
	Analizuje skuteczność różnych metod ochrony przed atakami, w tym stosowanie silnych haseł i zarządzania dostępem.	Test teoretyczny
Charakteryzuje dobre praktyki w pracy online i wdraża procedury ochrony danych osobowych oraz poufnych informacji.	Wyjaśnia zasady ochrony danych osobowych zgodne z RODO i innymi przepisami prawa.	Test teoretyczny
	Przeprowadza analizę procedur bezpiecznego korzystania z e-maili, w tym rozpoznawanie podejrzanych wiadomości i unikanie phishingu.	Test teoretyczny
	Opracowuje plan działania w przypadku wykrycia incydentu cybernetycznego.	Test teoretyczny
Monitoruje incydenty cybernetyczne i wdraża odpowiednie procedury reagowania.	Wdraża procedury reagowania na incydenty, takie jak zgłaszanie i dokumentowanie naruszeń bezpieczeństwa.	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

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

Tak

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

Tak

Program

MODUŁ I:

Wprowadzenie do cyberbezpieczeństwa

PRZERWA

MODUŁ II:

Rodzaje ataków cybernetycznych

PRZERWA

MODUŁ III:

Bezpieczne praktyki pracy online

PRZERWA

MODUŁ IV:

Bezpieczne korzystanie z e-maili

PRZERWA

MODUŁ V:

Ochrona danych osobowych i poufności informacji

PRZERWA

MODUŁ VI:

Reagowanie na incydenty cybernetyczne

MODUŁ VII:

Sesja Q&A

Harmonogram

Liczba przedmiotów/zajęć: 7

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 7 Wprowadzenie do cyberbezpieczeństwa	Jacek Kapelski	16-12-2024	08:00	09:00	01:00
2 z 7 Rodzaje ataków cybernetycznych	Jacek Kapelski	16-12-2024	09:00	10:30	01:30
3 z 7 Bezpieczne praktyki pracy online	Jacek Kapelski	16-12-2024	10:45	11:45	01:00
4 z 7 Bezpieczne korzystanie z e-maili	Jacek Kapelski	16-12-2024	11:45	12:45	01:00
5 z 7 Ochrona danych osobowych i poufności informacji	Jacek Kapelski	16-12-2024	13:00	14:30	01:30
6 z 7 Reagowanie na incydenty cybernetyczne	Jacek Kapelski	16-12-2024	14:30	15:30	01:00
7 z 7 Sesja Q&A	Jacek Kapelski	16-12-2024	15:30	16:00	00:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	960,00 PLN
Koszt przypadający na 1 uczestnika netto	780,49 PLN
Koszt osobogodziny brutto	120,00 PLN
Koszt osobogodziny netto	97,56 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Jacek Kapelski

Jacek Kapelski to doświadczony ekspert w dziedzinie cyberbezpieczeństwa, z pasją do technologii informatycznych, którą rozwijał przez wiele lat pracy w różnych sektorach IT. Jego kariera zawodowa rozpoczęła się w dużej korporacji, gdzie pełnił rolę administratora IT, zdobywając bezcenne doświadczenie w zarządzaniu rozbudowanymi infrastrukturami sieciowymi i serwerowymi. Dzięki swojej wiedzy i zaangażowaniu, Jacek szybko stał się nieocenionym członkiem zespołu odpowiedzialnego za bezpieczeństwo i stabilność systemów informatycznych firmy.

Jacek jest certyfikowanym specjalistą Windows Server, co potwierdza jego głęboką znajomość technologii Microsoft oraz umiejętność zarządzania serwerami na najwyższym poziomie. Jego podejście do cyberbezpieczeństwa cechuje się precyzją i dbałością o najmniejsze detale, co sprawia, że potrafi przewidzieć potencjalne zagrożenia i skutecznie im przeciwdziałać. Jacek wierzy, że kluczem do sukcesu w dzisiejszym cyfrowym świecie jest ciągłe doskonalenie umiejętności oraz poszerzanie wiedzy, co przekłada na swoje szkolenia, które prowadzi z pełnym zaangażowaniem i profesjonalizmem.

Prywatnie Jacek jest entuzjastą nowinek technologicznych i chętnie dzieli się swoją wiedzą z innymi, pomagając im lepiej zrozumieć skomplikowane zagadnienia związane z cyberbezpieczeństwem. Na jego szkoleniach uczestnicy mogą liczyć nie tylko na solidną dawkę wiedzy teoretycznej, ale także na praktyczne wskazówki i rozwiązania, które mogą od razu wdrożyć w swoich firmach.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymują: skrypt szkoleniowy, prezentację multimedialną, indywidualne długopisy, kartki i inne jednorazowe pomoce dydaktyczne a także certyfikat ukończenia szkolenia

Warunki uczestnictwa

- Uczestnikiem szkolenia może być każda osoba, która spełnia wymagania wiekowe oraz posiada podstawową wiedzę na temat systemów Windows oraz klientów pocztowych.
- Uczestnik powinien posiadać własny komputer przenośny z systemem Windows, który umożliwi mu praktyczne wykonywanie ćwiczeń podczas szkolenia.
- Uczestnicy powinni zachować odpowiedni poziom kultury i szacunku wobec prowadzącego oraz innych uczestników szkolenia.
- Organizator zapewnia oprogramowanie i środowisko testowe do przeprowadzania praktycznych ćwiczeń.

Informacje dodatkowe

Zawarto umowę z WUP w Toruniu w ramach Projektu Kierunek – Rozwój;

Adres

ul. Kijowska 44
85-703 Bydgoszcz

woj. kujawsko-pomorskie

Udogodnienia w miejscu realizacji usługi

- Wi-fi

Kontakt



Michał Majcherek

E-mail szkolenia@bps.edu.pl

Telefon (+48) 537 770 040