Możliwość dofinansowania

Cyberbezpieczeństwo - bezpieczeństwo cyfrowe

Numer usługi 2026/04/08/132102/3471684

885,60 PLN brutto
720,00 PLN netto
110,70 PLN brutto/h
90,00 PLN netto/h
261,33 PLN cena rynkowa

Empemedia Marcin Pietraszek

4,6 / 5

9 ocen

Usługa szkoleniowa
zdalna w czasie rzeczywistym
08:00 h
26.05.2026 do 26.05.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie JEST skierowane jest do pracowników "nie-technicznych", czyli do pracowników biurowych, którzy zajmują się m.in. obsługą klientów, administracją, marketingiem i w swojej pracy posiadają dostęp do Internetu. Szkolenie skierowane jest również do menedżerów oraz właścicieli firm. Szkolenie NIE jest skierowane do informatyków ani programistów.
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	21-05-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	8
Podstawa uzyskania wpisu do BUR	Znak Jakości Małopolskich Standardów Usług Edukacyjno-Szkoleniowych (MSUES) - wersja 2.0

Cel

Cel edukacyjny

Celem szkolenia jest nabycie przez uczestników wiedzy z zakresu ochrony informacji i cyberbezpieczeństwa w codziennej pracy biurowej.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik charakteryzuje prawne ramy bezpieczeństwa informacji i cyberbezpieczeństwa	Uczestnik poprawnie identyfikuje, które obowiązki prawne mają zastosowanie do danego typu organizacji	Test teoretyczny z wynikiem generowanym automatycznie
	Uczestnik wskazuje konsekwencje wynikające z niespełnienia obowiązków prawnych związanych z cyberbezpieczeństwem	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik definiuje pojęcie incydentu bezpieczeństwa informacji oraz opisuje zasady zarządzania incydentami w organizacji	Uczestnik prawidłowo klasyfikuje, czy dane zdarzenie stanowi incydent bezpieczeństwa	Test teoretyczny z wynikiem generowanym automatycznie
	Uczestnik prawidłowo wskazuje kolejne etapy procesu zarządzania incydentem bezpieczeństwa	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik rozpoznaje aktualne typy cyberataków, w szczególności phishing i ransomware, a także stosuje praktyczne metody weryfikacji podejrzanej korespondencji e-mail, linków i załączników z wykorzystaniem dostępnych narzędzi	Uczestnik poprawnie identyfikuje cechy charakterystyczne dla phishingu i odróżnia wiadomości autentyczne od fałszywych	Test teoretyczny z wynikiem generowanym automatycznie
	Uczestnik wybiera odpowiednie narzędzia lub metody służące do weryfikacji bezpieczeństwa otrzymanych linków lub załączników	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik stosuje zasady tworzenia i bezpiecznego zarządzania hasłami	Uczestnik buduje silne hasła	Test teoretyczny z wynikiem generowanym automatycznie
	Uczestnik wskazuje działania, jakie należy podjąć w przypadku stwierdzenia wycieku hasła	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Szkolenie odbywa się jednego dnia w godzinach **9:00 - 15:30** i jest realizowane zdalnie w czasie rzeczywistym:

- 8 godzin dydaktycznych (6 godzin zegarowych dziennie)
- przy czym 1 godzina dydaktyczna trwa 45 minut.

Przerwy - 30 minut - nie są wliczone w czas trwania usługi.

Metody pracy: wykład, prezentacja, udostępnianie ekranu, odpowiedzi na pytania Uczestników zadawane przez mikrofon lub czat tekstowy.

Walidacja wyników kształcenia odbywa się w formie testu teoretycznego z wynikiem generowanym automatycznie. Test (15 minut) jest wliczony do czasu szkolenia.

Warunki kształcenia. Szkolenie odbywa się na platformie LiveWebinar. Uczestnicy widzą trenera oraz prezentowane przez niego materiały (prezentacja, udostępniany podgląd omawianych aplikacji) i mogą zadawać pytania trenerowi przez mikrofon oraz na czacie. Każdy Uczestnik musi dysponować własnym urządzeniem (preferowany laptop/komputer) z dostępem do internetu oraz przeglądarki, a także kamerą i mikrofonem (więcej informacji znajduje się w zakładce "Warunki techniczne").

Prawne aspekty bezpieczeństwa informacji i cyberbezpieczeństwa

- Jakie mamy obowiązki w naszej organizacji?
- Czy dyrektywa NIS2 i nowa ustawa o KSC nas dotyczy?
- Czy RODO jeszcze działa?
- Wewnętrzne polityki procedury bezpieczeństwa to też prawo

Budowanie kultury bezpieczeństwa – kluczowe dla każdej organizacji

- Od czego zacząć?
- Czy człowiek to najsłabsze ogniwo?

Incydenty bezpieczeństwa

- Co to jest incydent?
- Kiedy i komu zgłaszać incydenty?
- Dlaczego warto zgłaszać incydenty?
- Jak zarządzać incydentami?

Aktualne zagrożenia w cyberprzestrzeni

- Typy ataków
- Popularne scenariusze
- Schematy działania cyberprzestępców
- Główne cyberzagrożenia
- Kradzieże i wyłudzenia informacji
- Jak się bronić?

Bezpieczna praca zdalna – dobre praktyki

Proste i skuteczne metody codziennej ochrony informacji przez pracowników

- Kopia bezpieczeństwa
- Szyfrowanie danych
- Blokowanie komputera
- Fizyczna ochrona urządzeń

Zagrożenia dla urządzeń mobilnych i zasady bezpiecznego korzystania

Audyty i testy bezpieczeństwa mają sens

- Rodzaje testów bezpieczeństwa
- Korzyści z testów
- Jak przygotować pracowników do testów socjotechnicznych?

Zasady bezpiecznego użytkowania poczty elektronicznej i mediów społecznościowych

Bezpieczne hasła do Twoich systemów

- Jak tworzyć silne hasła?
- Jakie hasła zawsze musimy mieć „w głowie”?
- Menedżery haseł, jako narzędzia do skutecznego zarządzania hasłami

Dwuskładnikowe uwierzytelnienie (2FA/MFA) to już standard w pracy i życiu prywatnym

Wycieki i kradzieże haseł

- Jak sprawdzić, czy moje hasła wyciekły?
- Co zrobić, gdy moje hasła wycieką?

Phishing i Ransomware jako największe zagrożenia dla każdej organizacji

- Jak odróżnić fałszywą korespondencję e-mail przychodzącą do naszej organizacji?
- Jak sprawdzić czy otrzymany link lub załącznik jest bezpieczny? Przykładowe narzędzia i zasady korzystania

Test teoretyczny z wynikiem generowanym automatycznie

Harmonogram

Liczba pozycji harmonogramu: 0

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Jeżeli korzystasz z dofinansowania w wysokości co najmniej 70% przysługuje Tobie zwolnienie z podatku VAT

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	885,60 PLN
Koszt przypadający na 1 uczestnika netto	720,00 PLN
Koszt osobogodziny brutto	110,70 PLN
Koszt osobogodziny netto	90,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

ARKADIUSZ STAWCZYK

Trener, doradca i kierownik projektów.

Specjalista w dziedzinie bezpieczeństwa informacji i cyberzagrożeń. Certyfikowany trener ECDL EPP e Urzędnik, egzaminator ECDL oraz kierownik projektów ICT (Fn-TSPM). Specjalista IT Security CISS (Certified IT Security Specialist). Poprzednio kierownik Wydziału Informatyki w dużej jednostce administracji samorządowej. Był odpowiedzialny za kluczowe projekty informatyczne realizowane w urzędzie oraz skuteczne wdrażanie Polityki Bezpieczeństwa Informacji. Pracował także jako kierownik wydziału serwisu w firmie z obszaru usług IT. Członek Polskiego Towarzystwa Informatycznego.

Doradza firmom i jednostkom administracji publicznej m.in. z zakresu ochrony informacji (tworzenie polityk bezpieczeństwa, instrukcji i procedur). Jest autorem licznych instrukcji i procedur związanych z ochroną danych osobowych i informacji. W zakresie szkoleń specjalizuje się w tematach związanych z informatyzacją administracji publicznej, cyberzagrożeniami, bezpieczeństwem informacji i ochroną danych osobowych (Rodo).

Posiada znajomość zarówno teoretyczną jak i praktyczną przedstawianych przez siebie tematów. Ma za sobą również kilkuletnie doświadczenie wykładowcy wyższej uczelni.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymują:

- prezentację (PDF)
- imienny Certyfikat Empemedia (PDF) z podpisem elektronicznym.

Warunki uczestnictwa

Wymogi dla Uczestników:

- Zalecamy logowanie za pośrednictwem indywidualnego linku przekazanego przed szkoleniem (każdy Uczestnik otrzymuje indywidualny link, przypisany do jego imienia, nazwiska, adresu e-mail).
- W przypadku, gdyby skorzystanie z indywidualnego linku było niemożliwe - wymagane jest podanie przy logowaniu pełnego imienia i nazwiska Uczestnika.
- Uczestnik powinien mieć włączoną kamerę przez całe szkolenie w celu weryfikacji obecności. Nagrania zostają zachowane do celów kontrolnych, ale nie są udostępniane uczestnikom.
- Uczestnik powinien wyrazić zgodę na utrwalenie i wykorzystanie jego wizerunku - w przypadku szkoleń z dofinansowaniem jest to warunek konieczny.
- Uczestnik, aby otrzymać Certyfikat, musi być obecny (zalogowany) przez minimum 80 lub 100% czasu trwania szkolenia - w zależności od wymagań programu.

Niespełnienie powyższych warunków może skutkować brakiem dofinansowania.

Warunki techniczne

Szkolenie może zostać zwolnione z VAT, o ile spełnione zostaną warunki ustawowe (finansowanie ze środków publicznych w min. 70%, szkolenie zawodowe).

Podstawa zwolnienia z VAT:

1) art. 43 ust. 1 pkt 29 lit. c Ustawy z dnia 11 marca 2024 o podatku od towarów i usług.

2) § 3 ust. 1 pkt. 14 Rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień.

W przypadku braku dofinansowania lub uzyskania dofinansowania poniżej 70%, do ceny netto doliczane jest 23% VAT

Kontakt

MARCIN PIETRASZEK

E-mail empe@empemedia.pl
Telefon (+48) 505 780 488