Możliwość dofinansowania

Szkolenie - Zapewnienie bezpieczeństwa cyfrowego organizacji: Bezpieczna praca w środowisku cyfrowym (Kwalifikacje)

Numer usługi 2026/05/04/41507/3532425

1 968,00 PLN brutto
1 600,00 PLN netto
246,00 PLN brutto/h
200,00 PLN netto/h
261,33 PLN cena rynkowa

Trustwise Sp. z o. o.

4,9 / 5

2 904 oceny

Rybnik
Usługa szkoleniowa
stacjonarna
08:00 h
16.06.2026 do 16.06.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie dedykowane jest dla wszystkich osób, które chcą rozwinąć swoje kompetencje i nabyć kwalifikacje w zakresie zapewnienia cyberbezpieczeństwa w organizacji, w szczególności zabezpieczenia firmy przed atakami hakerskimi, wypłynięciem danych z organizacji, zakłócenie działania firmy poprzez utratę danych i/lub sparaliżowanie systemów do zarządzania przedsiębiorstwem. Nie jest wymagana wcześniejsza specjalistyczna wiedza i umiejętności z zakresu szkolenia, natomiast pomocne w zrozumieniu tematyki szkolenia byłyby podstawowe umiejętności i kompetencje oraz znajomość systemów informatycznych klasy ERP stosowanych w firmie, obsługi komputera i poczty e-mail.
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	10
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	8
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

Szkolenie przygotowuje uczestników do identyfikowania potencjalnych zagrożeń w obszarze cyberbezpieczeństwa, wdrażania podstawowych mechanizmów ochronnych oraz skutecznego reagowania na incydenty związane z bezpieczeństwem informatycznym. Uczestnicy zdobywają wiedzę i umiejętności w zakresie praktycznego, odpowiedzialnego oraz bezpiecznego i ekologicznego zarządzania danymi i zasobami cyfrowymi, tak aby ich wykorzystanie w środowisku pracy było efektywne i zgodne z najlepszymi praktykami.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
W: Podaje znaczenie cyberbezpieczeństwa oraz jego wpływ na funkcjonowanie organizacji	Trafnie wskazuje pojęcie cyberbezpieczeństwa i podaje jego cele	Test teoretyczny z wynikiem generowanym automatycznie
	Trafnie wskazuje na wpływ bezpieczeństwa cyfrowego na funkcjonowanie organizacji	Test teoretyczny z wynikiem generowanym automatycznie
	Charakteryzuje główne zagrożenia cybernetyczne dla organizacji	Analiza dowodów i deklaracji
U: Zarządza i reaguje na incydenty wpływające na zagrożenie bezpieczeństwa	Opisuje etapy zarządzania incydentami bezpieczeństwa	Test teoretyczny z wynikiem generowanym automatycznie
	Analizuje przypadki i symulacje ataków	Analiza dowodów i deklaracji
	Podaje przykłady możliwych do zastosowania przez siebie i/lub stosowanych działań wpierających poprawę cyberbezpieczeństwa w firmie	Analiza dowodów i deklaracji
KS: Wspiera inicjatywy i działania mające na celu poprawę bezpieczeństwa cyfrowego organizacji	Aktywnie proponuje inicjatywy i działania mające na celu poprawę bezpieczeństwa cyfrowego organizacji	Analiza dowodów i deklaracji
	Współdziała na rzecz bezpieczeństwa informacji w miejscu pracy	Analiza dowodów i deklaracji
U: Rozpoznaje i reaguje na zagrożenia w cyberprzestrzeni (phishing, malware, ransomware)	Podejmuje właściwe reakcje na potencjalne cyberzagrożenia.	Analiza dowodów i deklaracji
	Podaje przykłady zagrożeń w cyberprzestrzeni	Analiza dowodów i deklaracji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
KS: Świadomie i odpowiedzialnie przetwarza dane osobowe	Definiuje pojęcia: dane osobowe, przetwarzanie, administrator danych, zgoda	Test teoretyczny z wynikiem generowanym automatycznie
	Wskazuje podstawy prawne przetwarzania danych oraz wymienia elementy ważnej zgody na przetwarzanie danych osobowych	Analiza dowodów i deklaracji
	Zna podstawowe pojęcia i przepisy RODO oraz obowiązki pracowników	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 dedykowane jest dla wszystkich osób, które chcą rozwinąć swoje kompetencje i nabyć kwalifikacje w obszarze identyfikowania potencjalnych zagrożeń w obszarze cyberbezpieczeństwa, wdrażania podstawowych mechanizmów ochronnych oraz skutecznego reagowania na incydenty związane z bezpieczeństwem informatycznym. Ważne, aby uczestnicy mieli możliwość po szkoleniu zastosowania poznanych dobrych praktyk, metod i narzędzi w praktyce, aby budowali pozytywne nawyki komunikacji i przepływu pracy.

Z uwagi na charakter szkolenia nie wymaga ono szczególnych warunków lokalowych i organizacyjnych. Dla efektywnego przeprowadzenia szkolenia wystarczająca będzie wyodrębniona sala szkoleniowa, najlepiej z dostępem do światła dziennego, wyposażona opcjonalnie w tablicę suchościeralną lub tablicę flipchart oraz ekran, na którym, za pośrednictwem rzutnika lub na ekranie, będą wyświetlane najważniejsze treści szkolenia i pokazywane zagadnienia. Każdy z uczestników powinien mieć zapewnione miejsce, przy którym będzie mógł wykonywać ćwiczenia lub notować prezentowane na w czasie szkolenia treści. Szkolenie realizowane jest w jednej grupie.

Warunkiem zrealizowania zakładanych celów edukacyjnych, **w tym nabycia cyfrowych kompetencji,** jest aktywny udział uczestników we wszystkich zadaniach i ćwiczeniach zespołowych, aktywne słuchanie i analiza przypadków omawianych podczas zajęć w celu zrozumienia i trwałego przyswojenia treści oraz nabycia zakładanej wiedzy, umiejętności i kompetencji, w tym kompetencji społecznych.

Zajęcia w dużej mierze będą realizowane metodami aktywnymi, rozumianymi jako metody umożliwiające uczenie się w oparciu o doświadczenie i pozwalające uczestnikom na ćwiczenie umiejętności i kompetencji.

Szkolenie będzie realizowane według poniższego programu:

Moduł 1: Podstawy cyberbezpieczeństwa

- - Wprowadzenie do pojęcia cyberbezpieczeństwa
  - Rola ochrony danych i zasobów technologicznych w zapewnieniu stabilności organizacji.
  - Przegląd najczęściej występujących zagrożeń w sieci i analiza ich wpływu na przedsiębiorstwa i użytkowników indywidualnych
  - Jak cyberataki oddziałują na funkcjonowanie przedsiębiorstwa
  - Dlaczego regularne aktualizacje oprogramowania są jednym z kluczowych sposobów ochrony danych.
- Zrozumienie znaczenia ochrony danych osobowych i prywatności oraz regulacji prawnych.

Moduł 2: Identyfikacja zagrożeń i skuteczna ochrona

- - Omówienie najpowszechniejszych rodzajów ataków, takich jak wirusy, phishing, ransomware, włamania sieciowe czy manipulacje socjotechniczne, oraz sposoby ich rozpoznawania z wykorzystaniem nowoczesnych narzędzi.
  - Zastosowanie programów antywirusowych i filtrów antyspamowych, które wspierają bezpieczne i jednocześnie efektywne korzystanie z zasobów technologicznych.
  - Znaczenie zapór sieciowych jako podstawowej bariery ochronnej, umożliwiającej stabilne działanie infrastruktury IT.
  - Wdrożenie szyfrowania danych jako metody długoterminowego i odpowiedzialnego podejścia do bezpieczeństwa informacji.
- Umiejętność stosowania bezpiecznych praktyk: tworzenie silnych haseł, dwuetapowa weryfikacja (MFA), wykonywanie kopii zapasowych, segmentacja sieci.
  - Kopie zapasowe – jak tworzyć je w sposób przemyślany

Moduł 3: Zarządzanie i reagowanie na incydenty

- - Jak rozpoznawać naruszenia bezpieczeństwa z pomocą inteligentnych narzędzi monitorujących w czasie rzeczywistym.
  - Skuteczne reagowanie na incydenty: procedury, analiza sytuacji, minimalizowanie szkód.
  - Strategie odbudowy po incydentach z użyciem rozwiązań wspierających sprawność działania organizacji.
  - Zapobieganie kolejnym atakom poprzez wdrażanie innowacyjnych technologii
  - Analiza realnych przypadków i symulacje ataków dla praktycznej nauki rozpoznawania i obrony.
  - Świadomość najczęstszych błędów użytkowników i sposobów ich unikania.

Szkolenie kończy się **możliwością uzyskania kwalifikacji: Zapewnienie bezpieczeństwa cyfrowego organizacji: Bezpieczna i skuteczna praca w środowisku cyfrowym** nadawanej przez Trustwise Sp. z o. o., firmę uznaną w wielu branżach i rekomendowaną przez pracodawców sektora usług cyfrowych oraz komunikacji online. Dokument potwierdzający uzyskanie kwalifikacji jest rozpoznawalny i uznawalny w wielu branżach i sektorach gospodarki a certyfikat otrzymał pozytywne rekomendacje od co najmniej 5 pracodawców danej branży/ sektorów lub związku branżowego, zrzeszającego pracodawców danej branży/sektorów.

Na szkolenie składa się 8 godzin lekcyjnych, powiększonych o przerwy uwzględnione w harmonogramie szkolenia. 1 godzina lekcyjna szkolenia to 45 minut. Liczba godzin teoretycznych: 4 godzin lekcyjnych; Liczba godzin praktycznych: 4 godziny lekcyjne.

Walidacja i certyfikacja:

Warunkiem uzyskania kwalifikacji jest uczestnictwo w co najmniej 80% zajęć oraz przejście przez proces walidacji. W ramach realizacji usługi edukacyjnej zostały wprowadzone **rozwiązania gwarantujące wyraźne oddzielenie procesu kształcenia i szkolenia od procesu walidacji.** Oznacza to, że osoba prowadząca szkolenie nie bierze udziału w ocenie ani weryfikacji efektów uczenia się uczestników.Pozytywny wynik walidacji skutkuje wydaniem certyfikatu potwierdzającego zdobycie kwalifikacji. Po szkoleniu trener rozdaje uczestnikom test z gotową kafeterią odpowiedzi do uzupełnienia, nie ingerując w jego wypełnienie. Następnie walidacja jest ustalana indywidualnie z Uczestnikiem usługi i odbędzie się w okresie od 1 do 5 dni od realizacji usługi.Termin walidacji dostępny będzie u osoby nadzorującej usługę po stronie Dostawcy Usług.

Certyfikacja polega na **formalnym potwierdzeniu** spełnienia wymagań oraz poprawności przeprowadzenia procesu walidacji. Decyzję certyfikacyjną podejmuje **osoba upoważniona przez instytucję**, **nieuczestnicząca w szkoleniu ani walidacji**, na podstawie kompletnej dokumentacji walidacyjnej. Certyfikat wydawany jest **wyłącznie po uzyskaniu pozytywnego wyniku walidacji**.

Instytucja stosuje **procedury zapewniające bezstronność**, w tym rozdział ról szkoleniowych, walidacyjnych i certyfikacyjnych oraz mechanizmy zapobiegania konfliktowi interesów. Uczestnikom przysługuje możliwość **złożenia odwołania** od wyniku walidacji zgodnie z obowiązującymi procedurami.

Zapewnienie dostępności: Zapewniamy równy dostęp do usługi dla wszystkich uczestników. Na prośbę uczestnika uzgadniamy równoważne formy materiałów i walidacji efektów (np. zastosowanie większej czcionki, wydłużenie czasu ekspozycji informacji lub wykorzystanie innych form przedstawienia danych, które umożliwiają lepsze ich zrozumienie i dostępność) bez obniżania kryteriów i progów zaliczenia.

Przy dofinansowaniu w wysokości co najmniej 70% szkolenie może zostać zwolnione z podatku VAT (na podstawie §3 ust.1 pkt 14 rozporządzenia Ministra Finansów z dnia 20.12.2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (Dz.U. z 2015 r., poz.736)). W przypadku braku otrzymania dofinansowania w zakładanej wysokości, cena zostanie powiększona o podatek VAT 23%.

Harmonogram

Liczba pozycji harmonogramu: 8

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 8 Podstawy cyberbezpieczeństwa	Adrian Panicz	16-06-2026	08:00	09:30	01:30
2 z 8 Przerwa	Adrian Panicz	16-06-2026	09:30	09:40	00:10
3 z 8 Identyfikacja zagrożeń	Adrian Panicz	16-06-2026	09:40	11:25	01:45
4 z 8 Przerwa	Adrian Panicz	16-06-2026	11:25	11:35	00:10
5 z 8 Skuteczna ochrona przed zagrożeniami	Adrian Panicz	16-06-2026	11:35	12:50	01:15
6 z 8 Przerwa	Adrian Panicz	16-06-2026	12:50	13:10	00:20
7 z 8 Zarządzanie i reagowanie na incydenty	Adrian Panicz	16-06-2026	13:10	14:40	01:30
8 z 8 Walidacja (test teoretyczny z wynikiem generowanym automatycznie, wywiad swobodny, analiza dowodów i deklaracji)	-	16-06-2026	14:40	14:55	00:15

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	1 968,00 PLN
Koszt przypadający na 1 uczestnika netto	1 600,00 PLN
Koszt osobogodziny brutto	246,00 PLN
Koszt osobogodziny netto	200,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Adrian Panicz

Doświadczony trener i wdrożeniowiec systemów do zarządzania przedsiębiorstwem klasy ERP, oraz systemów CRM i DMS. Konsultant firm przy wdrażaniu rozwiązań usprawniających funkcjonowanie biznesu w różnych jego aspektach - zarządzanie, zarządzanie projektami, sprzedaż, logistyka, produkcja, magazyn. Na jego doświadczenie składa się ponad 13 lat pracy zawodowej, ponad 140 wdrożeń i ponad 670 dni szkoleniowych na przestrzeni ostatnich 7 lat. Z pasji i zamiłowania informatyk. Posiada wykształcenie wyższe.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy uczestnik otrzyma notes, długopis oraz e-podręcznik z najważniejszymi treściami szkolenia.

Informacje dodatkowe

Walidacja i certyfikacja:

Warunkiem uzyskania kwalifikacji jest uczestnictwo w co najmniej 80% zajęć oraz przejście przez proces walidacji. W ramach realizacji usługi edukacyjnej zostały **wprowadzone rozwiązania gwarantujące wyraźne oddzielenie procesu kształcenia i szkolenia od procesu walidacji.** Oznacza to, że osoba prowadząca szkolenie nie bierze udziału w ocenie ani weryfikacji efektów uczenia się uczestników. Pozytywny wynik walidacji skutkuje **wydaniem certyfikatu potwierdzającego zdobycie kwalifikacji.** „Walidacja jest ustalana indywidualnie z Uczestnikiem usługi i odbędzie się w okresie od 1 do 5 dni od realizacji usługi.Termin walidacji dostępny będzie u osoby nadzorującej usługę po stronie Dostawcy Usług.

Adres

ul. Bolesława Chrobrego 21

44-200 Rybnik

woj. śląskie

Informacja o dostępności:
W przypadku chęci zgłoszenia uwag i sugestii dotyczących warunków lokalowych miejsca, w którym odbywa się szkolenie, związanych z zapewnieniem dostępności do udziału w usłudze, prosimy o kontakt z koordynatorem projektu: Jakub Walczak, jakub.walczak@trustwise.com.pl, (+48) 22 398 79 45

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi

Kontakt

Jakub Walczak

E-mail jakub.walczak@trustwise.com.pl

Telefon (+48) 223 987 945