Możliwość dofinansowania

C4Y KATARZYNA ZASIECZNA

Brak ocen dla tego dostawcy

Cyberbezpieczeństwo w firmie usługowej – ochrona firmy, pracowników i klientów przed zagrożeniami

Numer usługi 2026/09/15/203083/3812194

Poznań
Usługa szkoleniowa
stacjonarna
Zajęcia grupowe
08:00 h
26.10.2026 do 26.10.2026

2 829,00 PLN brutto
2 300,00 PLN netto
353,63 PLN brutto/h
287,50 PLN netto/h
266,67 PLN cena rynkowa

Informacje podstawowe

Kategoria	Techniczne / Pozostałe techniczne
Grupa docelowa usługi	Grupę docelową usługi stanowią właściciele, współwłaściciele, kadra zarządzająca oraz pracownicy firm usługowych, w szczególności przedsiębiorstw świadczących usługi sprzątania i utrzymania czystości. Szkolenie skierowane jest do osób odpowiedzialnych za korzystanie z poczty elektronicznej, urządzeń służbowych, nadawanie i kontrolę dostępów pracowników oraz ochronę danych klientów. Uczestnikami mogą być również przedsiębiorcy współpracujący z klientami wymagającymi stosowania podstawowych standardów cyberbezpieczeństwa. Wymagana jest podstawowa umiejętność korzystania z poczty elektronicznej, telefonu i komputera. Nie jest wymagane wykształcenie informatyczne ani specjalistyczna wiedza techniczna.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	5
Data zakończenia rekrutacji	25-10-2026
Forma prowadzenia usługi	stacjonarna
Podstawa uzyskania wpisu do BUR	Znak Jakości TGLS Quality Alliance

Cel

Cel edukacyjny

Usługa przygotuje uczestnika do samodzielnego rozpoznawania najczęstszych cyberzagrożeń oraz bezpiecznego organizowania korzystania z kont, urządzeń i danych w małej firmie usługowej. Uczestnik nauczy się rozpoznawać phishing, BEC, fałszywe faktury, zagrożenia wykorzystujące AI i deepfake, stosować hasła i MFA, zabezpieczać urządzenia, pocztę, chmurę i kopie zapasowe oraz właściwie reagować na przejęcie konta lub utratę urządzenia.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Identyfikuje cyberzagrożenia	rozpoznaje phishing, BEC, przejęcie konta i ransomware	Wywiad swobodny
Organizuje bezpieczne logowanie	uzasadnia dobór MFA i zasad zarządzania hasłami	Wywiad swobodny
Zarządza uprawnieniami	opracowuje sposób nadawania i odbierania dostępu	Wywiad swobodny
Dobiera zabezpieczenia urządzeń	wskazuje zabezpieczenia telefonu lub laptopa adekwatne do ryzyka	Wywiad swobodny
Rozpoznaje zagrożenia AI	identyfikuje deepfake, klonowanie głosu i phishing wspomagany AI	Wywiad swobodny
Reaguje na cyberincydent	wykonuje prawidłową sekwencję działań po przejęciu konta lub utracie urządzenia	Wywiad swobodny

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

Grupę docelową usługi stanowią właściciele, współwłaściciele, kadra zarządzająca oraz pracownicy firm usługowych, w szczególności przedsiębiorstw świadczących usługi sprzątania i utrzymania czystości. Szkolenie skierowane jest do osób odpowiedzialnych za korzystanie z poczty elektronicznej, urządzeń służbowych, nadawanie i kontrolę dostępów pracowników oraz ochronę danych klientów. Uczestnikami mogą być również przedsiębiorcy współpracujący z klientami wymagającymi stosowania podstawowych standardów cyberbezpieczeństwa. Wymagana jest podstawowa umiejętność korzystania z poczty elektronicznej, telefonu i komputera. Nie jest wymagane wykształcenie informatyczne ani specjalistyczna wiedza techniczna.

Usługa przygotuje uczestnika do samodzielnego rozpoznawania najczęstszych cyberzagrożeń oraz bezpiecznego organizowania korzystania z kont, urządzeń i danych w małej firmie usługowej. Uczestnik nauczy się rozpoznawać phishing, BEC, fałszywe faktury, zagrożenia wykorzystujące AI i deepfake, stosować hasła i MFA, zabezpieczać urządzenia, pocztę, chmurę i kopie zapasowe oraz właściwie reagować na przejęcie konta lub utratę urządzenia.

Zakres tematyczny szkolenia:

Moduł 1. Najczęstsze cyberzagrożenia dla firmy usługowej

- phishing, spear phishing i wyłudzanie danych
- Business Email Compromise i podszywanie się pod klienta lub właściciela
- fałszywe faktury i próby zmiany numeru rachunku
- przejęcie skrzynki e-mail, komunikatora lub konta chmurowego
- ransomware i utrata dostępności danych

Moduł 2. Konta, hasła, MFA i urządzenia

- zasady tworzenia i przechowywania haseł
- uwierzytelnianie wieloskładnikowe
- zasada najmniejszych uprawnień
- nadawanie i odbieranie dostępów
- telefon i laptop pracownika – blokada, aktualizacje, szyfrowanie

Moduł 3. Poczta, chmura, komunikatory i dane klientów

- bezpieczna poczta i weryfikacja nietypowych dyspozycji
- udostępnianie plików i linków w chmurze
- WhatsApp, Messenger i inne komunikatory służbowe
- bezpieczne wykonywanie i przesyłanie zdjęć z realizacji
- kopie zapasowe i podstawowe zasady odtwarzania danych

Moduł 4. AI, deepfake i nowe formy socjotechniki

- wykorzystanie generatywnej AI przez cyberprzestępców
- deepfake obrazu i wideo oraz klonowanie głosu
- podszywanie się pod klienta, właściciela lub pracownika
- weryfikacja nietypowych dyspozycji i zmian danych płatniczych
- bezpieczne korzystanie z narzędzi AI przez pracowników

Moduł 5. Warsztat: cyberincydent i plan zabezpieczeń

- symulacja przejęcia skrzynki e-mail lub telefonu
- ustalenie kolejności działań po incydencie
- zmiana danych uwierzytelniających i odcięcie dostępu
- dokumentowanie zdarzenia i komunikacja z klientem
- ocena, czy cyberincydent może być naruszeniem danych osobowych
- przygotowanie indywidualnej checklisty bezpieczeństwa

Rezultat modułu/warsztatu: checklista minimalnych zabezpieczeń i schemat reakcji na cyberincydent.

Walidacja (15 minut)

Walidacja odbędzie się poprzez wywiad swobodny z kursantami oraz obserwację w warunkach rzeczywistych. Osoba przeprowadzająca walidacje dołączy pod koniec warsztatu. Osoba walidująca będzie obecna na sali, obserwując prace uczestniczek, nie ingerując w proces edukacyjny. Po części edukacyjnej osoba walidująca przeprowadzi z kursantami wywiad swobodny. Na wywiad swobodny przewidziane jest 15

minut na każdego uczestnika.

Obecność kursanta sprawdzana jest na podstawie listy obecności.

Usługa prowadzona jest maksymalnie w grupie 5 osobowej. W czasie trwania szkolenia kursanci siedzą przy stole podczas, gdy wykładowca omawia prezentację wyświetlaną na telewizorze.

Harmonogram

Liczba pozycji harmonogramu: 11

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 11 Moduł 1. Najczęstsze cyberzagrożenia dla firmy usługowej	Zajęcia	KATARZYNA ZASIECZNA	26-10-2026	09:00	10:15	01:15
2 z 11 -	Przerwa	-	26-10-2026	10:15	10:25	00:10
3 z 11 Moduł 2. Konta, hasła, MFA i bezpieczeństwo urządzeń	Zajęcia	KATARZYNA ZASIECZNA	26-10-2026	10:25	11:40	01:15
4 z 11 -	Przerwa	-	26-10-2026	11:40	11:50	00:10
5 z 11 Moduł 3. Bezpieczeństwo poczty, chmury, komunikatorów i danych klientów	Zajęcia	KATARZYNA ZASIECZNA	26-10-2026	11:50	13:05	01:15
6 z 11 -	Przerwa	-	26-10-2026	13:05	13:25	00:20
7 z 11 Moduł 4. AI, deepfake i nowe formy socjotechniki	Zajęcia	KATARZYNA ZASIECZNA	26-10-2026	13:25	14:40	01:15
8 z 11 -	Przerwa	-	26-10-2026	14:40	14:50	00:10

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
9 z 11 Moduł 5. Warsztat: cyberincydent i plan zabezpieczeń firmy	Zajęcia	KATARZYNA ZASIECZNA	26-10-2026	14:50	16:35	01:45
10 z 11 -	Przerwa	-	26-10-2026	16:35	16:45	00:10
11 z 11 -	Walidacja	-	26-10-2026	16:45	17:00	00:15

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	08:00
w tym suma godzin zajęć	06:45
w tym suma godzin walidacji	00:15
w tym suma przerw	01:00
Suma godzin dydaktycznych bez przerw	09:15

Cennik

Jeżeli korzystasz z dofinansowania i usługa stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego wraz z usługą lub dostawą towarów ściśle związaną z usługami kształcenia zawodowego lub przekwalifikowania zawodowego to możesz mieć możliwość skorzystania za zwolnienia z podatku VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług, jeśli usługa w całości jest finansowana ze środków publicznych lub § 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, gdy usługa jest finansowana w co najmniej 70% ze środków publicznych.

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 829,00 PLN
Koszt przypadający na 1 uczestnika netto	2 300,00 PLN
Koszt osobogodziny brutto	353,63 PLN

Koszt osobogodziny netto	287,50 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	08:00

Prowadzący

Liczba prowadzących: 1

1 z 1

KATARZYNA ZASIECZNA

Ekspertka ds. bezpieczeństwa informacji i ochrony danych osobowych (RODO). Od 2010 r. pełniła funkcję Administratora Bezpieczeństwa Informacji (ABI), odpowiadając za dokumentację, procedury i nadzór nad ochroną danych. Od 2015 r. prowadzi działalność szkoleniowo-doradczą, realizując wdrożenia, audyty, porządkowanie dokumentacji, szkolenia oraz bieżące wsparcie organizacji w zakresie RODO i bezpieczeństwa informacji. Absolwentka kierunków:
Administrator Bezpieczeństwa Informacji (ABI) na Wyższa Szkoła Administracji Publicznej w Szczecinie (2015)
Ochrona Danych Osobowych - Uniwersytet Wrocławski, Wydział Prawa, Administracji i Ekonomii (2018).
Od 2018 r. działa jako Inspektor Ochrony Danych (IOD) w sektorze publicznym i prywatnym (m.in. jednostki budżetowe, OPS, wodociągi, szkoły i przedszkola, dealerzy samochodowi, kliniki i podmioty lecznicze), w tym: monitoruje zgodność, prowadzi szkolenia, wspiera analizy ryzyka, obsługę naruszeń i incydentów oraz współpracę z IT i podmiotami przetwarzającymi. Specjalizuje się w podejściu proceduralnym do cyberbezpieczeństwa: polityki bezpieczeństwa, dokumentacja, audyty SZBI wg ISO/IEC 27001, RODO, reakcja na incydenty i budowanie odporności organizacji.
Doświadczenie szkoleniowe: 1694 godziny dydaktyczne.
Doświadczenie i kwalifikacje zdobyte w ciąghu soatatnuch 5 lat od daty publikacji usługi.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymają:

- materiały szkoleniowe
- checklistę analizy procesów przetwarzania danych,
- checklistę marketingu i zgód,
- checklistę podstaw cyberbezpieczeństwa w małej firmie,
- schemat postępowania w przypadku incydentu lub naruszenia danych.

Informacje dodatkowe

Zapisując się na usługę wyrażasz zgodę na rejestrowanie/nagrywanie swojego wizerunku na potrzeby monitoringu, kontroli oraz w celu utrwalenia efektów uczenia się.

Usługa może być zwolniona z VAT dla Uczestników, których poziom dofinansowania wynosi co najmniej 70% na podstawie § 3 ust. 1 pkt. 14 Rozporządzenia Ministrów Finansów z 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień.

Adres

ul. Pokrzywno 3D

61-315 Poznań

woj. wielkopolskie

Pokrzywno 3D, 61-315 Poznań

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi

Kontakt

KATARZYNA ZASIECZNA

E-mail katarzynazasieczna@gmail.com

Telefon (+48) 668 163 580