



C4Y KATARZYNA
ZASIECZNA

Brak ocen dla tego dostawcy

Szkolenie: Cyberbezpieczeństwo w Praktyce - Zarządzanie Incydentami/Ochrona Danych/ AI / Bezpieczeństwo Cyfrowych Procesów Marketingowych.

Numer usługi 2026/08/27/203083/3771789

- Poznań
- Usługa szkoleniowa
- stacjonarna
- Zajęcia grupowe
- 16:00 h
- 09.11.2026 do 10.11.2026

5 658,00 PLN brutto
4 600,00 PLN netto
353,63 PLN brutto/h
287,50 PLN netto/h
261,33 PLN cena rynkowa ⓘ

Informacje podstawowe

Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

Grupa docelowa usługi

Grupę docelową usługi stanowią osoby zawodowo związane z tworzeniem, produkcją, publikacją i dystrybucją treści cyfrowych oraz zarządzaniem zasobami wykorzystywanymi w marketingu, branży kreatywnej i produkcji audiowizualnej, w szczególności właściciele i pracownicy agencji marketingowych, reklamowych, kreatywnych i social media, producenci, operatorzy, montażyści, fotografowie, graficy, copywriterzy, content managerowie i social media managerowie, a także osoby odpowiedzialne za obsługę kont reklamowych, profili społecznościowych, stron internetowych, systemów CMS, usług chmurowych oraz współpracę z klientami i podwykonawcami. Szkolenie jest również skierowane do osób odpowiedzialnych za bezpieczeństwo informacji, ochronę danych osobowych, zarządzanie dostępami do zasobów cyfrowych oraz reagowanie na incydenty cyberbezpieczeństwa w organizacji.

Minimalna liczba uczestników

2

Maksymalna liczba uczestników

5

Data zakończenia rekrutacji

08-11-2026

Forma prowadzenia usługi

stacjonarna

Podstawa uzyskania wpisu do BUR

Znak Jakości TGLS Quality Alliance

Cel

Cel edukacyjny

Usługa dostarczy uczestnikowi wiedzy i praktycznych umiejętności w zakresie identyfikowania zagrożeń cyberbezpieczeństwa, ochrony kont, urządzeń, danych i zasobów cyfrowych oraz reagowania na incydenty. Uczestnik nauczy się oceniać incydenty pod kątem RODO, rozpoznawać ryzyka związane z AI i deepfake oraz stosować podstawowe procedury i zasady bezpieczeństwa w działalności marketingowej i produkcji treści.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Identyfikuje i ocenia zagrożenia cyberbezpieczeństwa występujące w marketingu i produkcji treści	rozpoznaje phishing, spear phishing, BEC oraz próby podszywania się; identyfikuje zagrożenia dotyczące poczty elektronicznej, kont użytkowników, kont social media i kont reklamowych; rozpoznaje sygnały ostrzegawcze świadczące o możliwym ataku; identyfikuje ryzyka związane z generatywną AI, deepfake i klonowaniem głosu	Wywiad swobodny
Stosuje zasady bezpiecznego zarządzania kontami, dostępami, urządzeniami oraz cyfrowymi zasobami organizacji	stosuje zasady MFA, bezpiecznego zarządzania hasłami i zasadę najmniejszych uprawnień; określa zasady nadawania, weryfikowania i odbierania dostępów; dobiera sposób bezpiecznego przechowywania i udostępniania plików oraz materiałów; wskazuje zasady wykonywania kopii zapasowych i podstawowego zabezpieczania urządzeń	Wywiad swobodny
Przeprowadza analizę poziomu cyberbezpieczeństwa organizacji i identyfikuje działania wymagające wdrożenia	identyfikuje nieprawidłowości w zarządzaniu dostępami, kontami i plikami; wskazuje brakujące zabezpieczenia; analizuje ryzyka związane ze współpracą z pracownikami i podwykonawcami; określa priorytetowe działania zwiększające poziom bezpieczeństwa; przygotowuje checklistę bezpieczeństwa organizacji	Obserwacja w warunkach rzeczywistych
Reaguje na incydent cyberbezpieczeństwa i ocenia jego wpływ na bezpieczeństwo danych osobowych	identyfikuje i klasyfikuje zdarzenie; określa jego potencjalny zakres; ustala kolejność działań; wskazuje zasoby wymagające zabezpieczenia; rozróżnia incydent cyberbezpieczeństwa od naruszenia ochrony danych osobowych; ocenia możliwość naruszenia poufności, integralności lub dostępności danych; określa działania wymagane po wystąpieniu zdarzenia	Obserwacja w warunkach rzeczywistych

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Opracowuje podstawowe procedury i rozwiązania organizacyjne wspierające cyberbezpieczeństwo organizacji	przygotowuje zasady nadawania i odbierania dostępów; określa zasady reagowania na incydenty, wykonywania kopii zapasowych i współpracy z podwykonawcami; uwzględnia podstawowe zasady bezpiecznego korzystania z AI; przygotowuje checklistę reagowania na incydent i określa dalsze działania organizacyjne	Obserwacja w warunkach rzeczywistych

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

TAK

Pytanie 2. Czy dokument lub wyrażnie 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 wyrażnie 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 osoby zawodowo związane z tworzeniem, produkcją, publikacją i dystrybucją treści cyfrowych oraz zarządzaniem zasobami wykorzystywanymi w marketingu, branży kreatywnej i produkcji audiowizualnej, w szczególności właściciele i pracownicy agencji marketingowych, reklamowych, kreatywnych i social media, producenci, operatorzy, montażyści, fotografowie, graficy, copywriterzy, content managerowie i social media managerowie, a także osoby odpowiedzialne za obsługę kont reklamowych, profili społecznościowych, stron internetowych, systemów CMS, usług chmurowych oraz współpracę z klientami i podwykonawcami. Szkolenie jest również skierowane do osób odpowiedzialnych za bezpieczeństwo informacji, ochronę danych osobowych, zarządzanie dostępami do zasobów cyfrowych oraz reagowanie na incydenty cyberbezpieczeństwa w organizacji.

Usługa dostarczy uczestnikowi wiedzy i praktycznych umiejętności w zakresie identyfikowania zagrożeń cyberbezpieczeństwa, ochrony kont, urządzeń, danych i zasobów cyfrowych oraz reagowania na incydenty. Uczestnik nauczy się oceniać incydenty pod kątem RODO, rozpoznawać ryzyka związane z AI i deepfake oraz stosować podstawowe procedury i zasady bezpieczeństwa w działalności marketingowej i produkcji treści.

Zakres tematyczny szkolenia:

DZIEŃ 1 – Ochrona organizacji, kont, danych i cyfrowych zasobów

Moduł 1. Zaawansowane cyberzagrożenia w marketingu i produkcji treści

- współczesne modele ataków na firmy z branży kreatywnej i marketingowej,
- phishing i spear phishing,
- Business Email Compromise (BEC),
- podszywanie się pod klienta, przełożonego, pracownika lub kontrahenta,
- próby zmiany numeru rachunku bankowego i fałszywe faktury,
- przejmowanie skrzynek pocztowych,
- przejmowanie profili social media i kont reklamowych,
- wyłudzenie danych uwierzytelniających,
- identyfikacja sygnałów ostrzegawczych wskazujących na atak.

Moduł 2. Bezpieczeństwo kont, dostępów i urządzeń

- uwierzytelnianie wieloskładnikowe – MFA,
- zasady tworzenia i przechowywania haseł,
- wykorzystanie menedżerów haseł,
- zasada najmniejszych uprawnień,
- indywidualne i współdzielone konta użytkowników,
- nadawanie dostępu pracownikom i podwykonawcom,
- okresowa weryfikacja uprawnień,
- odbieranie dostępów po zakończeniu współpracy,
- bezpieczeństwo komputerów i urządzeń mobilnych,
- aktualizacje oprogramowania i podstawowe zabezpieczenia urządzeń.

Moduł 3. Bezpieczeństwo chmury, plików i materiałów produkcyjnych

- bezpieczne przechowywanie zdjęć, nagrań, projektów i materiałów klientów,
- zasady korzystania z dysków współdzielonych i usług chmurowych,
- bezpieczne przekazywanie dużych plików,
- kontrola dostępu do materiałów przed publikacją,
- linki publiczne i udostępnianie zasobów,
- ochrona informacji poufnych i materiałów nieopublikowanych,
- kopie zapasowe,
- podstawowe zasady odtwarzania danych,
- ograniczanie skutków utraty lub zaszyfrowania danych.

Warsztat 1. Audyt bezpieczeństwa przykładowej firmy marketingowej

- identyfikacja nieprawidłowości w sposobie zarządzania dostępami,
- analiza zagrożeń dotyczących poczty i kont użytkowników,
- identyfikacja nieprawidłowego udostępniania plików,
- wskazanie brakujących zabezpieczeń,
- analiza ryzyk związanych ze współpracą z podwykonawcami,
- określenie działań, które powinny zostać wdrożone w pierwszej kolejności,
- przygotowanie checklisty bezpieczeństwa organizacji.

Walidacja (15 minut)

DZIEŃ 2 – Incydenty, RODO, AI i procedury bezpieczeństwa

Moduł 4. Reagowanie na incydenty cyberbezpieczeństwa

- czym jest incydent cyberbezpieczeństwa,
- identyfikacja i wstępna klasyfikacja zdarzenia,
- pierwsze działania po wykryciu incydentu,
- zabezpieczenie konta lub urządzenia,
- zmiana danych uwierzytelniających,
- ograniczenie dostępu,
- zabezpieczanie informacji o zdarzeniu i dowodów,
- ustalanie zakresu incydentu,
- dokumentowanie przebiegu zdarzenia,
- komunikacja z klientem, pracownikami i podwykonawcami,
- działania naprawcze po zakończeniu incydentu.

Moduł 5. Cyberincydent a naruszenie ochrony danych osobowych

- różnica pomiędzy incydemem bezpieczeństwa a naruszeniem ochrony danych osobowych,
- naruszenie poufności, integralności i dostępności danych,
- ocena skutków zdarzenia,
- analiza ryzyka dla praw i wolności osób fizycznych,
- dokumentowanie naruszeń,
- przesłanki zgłoszenia naruszenia Prezesowi UODO,
- termin 72 godzin,
- zawiadomienie osoby, której dane dotyczą,
- informacje wymagane przy dokumentowaniu zdarzenia,
- praktyczne przykłady naruszeń występujących w marketingu i produkcji treści.

Moduł 6. AI, deepfake i nowe cyberzagrożenia

- wykorzystanie generatywnej AI przez cyberprzestępców,
- automatyzacja phishingu,
- tworzenie wiarygodnych fałszywych wiadomości,
- klonowanie głosu,
- deepfake obrazu i wideo,
- podszywanie się pod członków kierownictwa, klientów i kontrahentów,
- weryfikacja nietypowych dyspozycji,
- bezpieczne wykorzystywanie narzędzi AI przez pracowników,
- ryzyko przekazywania danych osobowych i informacji poufnych do narzędzi AI,
- podstawowe zasady wewnętrznej polityki korzystania z AI.

Moduł 7. System cyberbezpieczeństwa w małej i średniej organizacji

- podział odpowiedzialności za bezpieczeństwo,
- procedura nadawania i odbierania dostępów,
- procedura reagowania na incydenty,
- zasady wykonywania kopii zapasowych,
- zarządzanie urządzeniami,
- zasady pracy zdalnej,
- bezpieczeństwo współpracy z podwykonawcami,
- minimalny zestaw zabezpieczeń organizacyjnych,
- tworzenie checklisty reagowania na incydent,
- budowanie świadomości pracowników.

Warsztat 2. Symulacja incydentu

Scenariusz przykładowy: przejęcie skrzynki e-mail pracownika oraz konta reklamowego klienta po skutecznym ataku phishingowym.

- identyfikacja zdarzenia,
- określenie potencjalnego zakresu incydentu,
- ustalenie kolejności działań,
- wskazanie zasobów wymagających zabezpieczenia,
- ocena, czy mogło dojść do naruszenia ochrony danych osobowych,
- wskazanie dalszych działań organizacyjnych,
- przygotowanie checklisty reagowania na incydent.

Walidacja (15 minut)

Walidacja odbędzie się poprzez wywiad swobodny z kursantami oraz obserwację w warunkach rzeczywistych. Osoba przeprowadzająca walidację 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: 16

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 16 Zaawansowane cyberzagrożenia w marketingu i produkcji treści	Zajęcia	KATARZYNA ZASIECZNA	09-11-2026	09:00	10:30	01:30
2 z 16 -	Przerwa	-	09-11-2026	10:30	10:45	00:15
3 z 16 Moduł 2. Bezpieczeństwo kont, dostępów i urządzeń	Zajęcia	KATARZYNA ZASIECZNA	09-11-2026	10:45	12:15	01:30
4 z 16 -	Przerwa	-	09-11-2026	12:15	12:45	00:30
5 z 16 Moduł 3. Bezpieczeństwo chmury, plików i materiałów produkcyjnych	Zajęcia	KATARZYNA ZASIECZNA	09-11-2026	12:45	14:15	01:30
6 z 16 -	Przerwa	-	09-11-2026	14:15	14:30	00:15
7 z 16 Warsztat 1. Audyt bezpieczeństwa przykładowej firmy marketingowej	Zajęcia	KATARZYNA ZASIECZNA	09-11-2026	14:30	16:45	02:15
8 z 16 -	Walidacja	-	09-11-2026	16:45	17:00	00:15
9 z 16 Reagowanie na incydenty cyberbezpieczeństwa	Zajęcia	KATARZYNA ZASIECZNA	10-11-2026	09:00	10:30	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
10 z 16 -	Przerwa	-	10-11-2026	10:30	10:45	00:15
11 z 16 Moduł 5. Cyberincydent a naruszenie ochrony danych osobowych	Zajęcia	KATARZYNA ZASIECZNA	10-11-2026	10:45	12:15	01:30
12 z 16 -	Przerwa	-	10-11-2026	12:15	12:45	00:30
13 z 16 Moduł 6. AI, deepfake i nowe cyberzagrożenia	Zajęcia	KATARZYNA ZASIECZNA	10-11-2026	12:45	14:30	01:45
14 z 16 -	Przerwa	-	10-11-2026	14:30	14:45	00:15
15 z 16 Moduł 7. System cyberbezpieczeństwa w małej i średniej organizacji + Warsztat 2. Symulacja incydentu	Zajęcia	KATARZYNA ZASIECZNA	10-11-2026	14:45	16:45	02:00
16 z 16 -	Walidacja	-	10-11-2026	16:45	17:00	00:15

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	16:00
w tym suma godzin zajęć	13:30
w tym suma godzin walidacji	00:30
w tym suma przerw	02:00
Suma godzin dydaktycznych bez przerw	18:30

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, jeżeli 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	5 658,00 PLN
Koszt przypadający na 1 uczestnika netto	4 600,00 PLN
Koszt osobogodziny brutto	353,63 PLN
Koszt osobogodziny netto	287,50 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	16:00

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 ciągu ostatnich 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