



AD-TRADE SPÓŁKA
Z OGRANICZONĄ
ODPOWIEDZIALNOŚ
CIĄ

Brak ocen dla tego dostawcy

Stosowanie zasad bezpiecznego przetwarzania, przechowywania i udostępniania danych w codziennej pracy

Numer usługi 2026/09/07/205802/3794199

- 📄 Usługa szkoleniowa
- 📺 zdalna w czasie rzeczywistym
- 👥 Zajęcia grupowe
- 🕒 16:00 h
- 📅 12.01.2027 do 13.01.2027

2 080,00 PLN brutto
2 080,00 PLN netto
130,00 PLN brutto/h
130,00 PLN netto/h
261,33 PLN cena rynkowa ⓘ

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie skierowane jest do pracowników mikro, małych i średnich przedsiębiorstw ze wszystkich branż, w szczególności do firm sektora finansowego i ubezpieczeniowego (PKD sekcja K, działy 64, 65 i 66) – banków, w tym banków spółdzielczych, SKOK, zakładów ubezpieczeń, agencji i multiagencji ubezpieczeniowych, brokerów, pośredników kredytowych, firm pożyczkowych, leasingowych i faktoringowych, domów maklerskich, TFI oraz podmiotów świadczących działalność wspomagającą usługi finansowe. Adresatami są wszyscy pracownicy korzystający w pracy z poczty elektronicznej, komputera lub telefonu służbowego: obsługa klienta, sprzedaż, księgowość, kadry, zaplecze operacyjne, kadra kierownicza oraz właściciele firm. Usługa nie jest adresowana do personelu IT i nie wymaga wiedzy informatycznej ani przygotowania technicznego.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	05-01-2027
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
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

Usługa przygotowuje pracownika MŚP do bezpiecznego przetwarzania, przechowywania i udostępniania danych. Uczestnik rozróżnia kategorie danych i przypisuje im poziomy poufności, identyfikuje dane krytyczne dla ciągłości działania, stosuje zasadę przetwarzania wyłącznie danych niezbędnych, szyfruje pliki, korzysta z bezpiecznych platform transferu, rozpoznaje sytuacje mogące prowadzić do wycieku danych i zna zakres swojej odpowiedzialności.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
4.1. Charakteryzuje rodzaje danych i informacji w przedsiębiorstwie	Rozróżnia kategorie danych, w tym dane osobowe i finansowe; definiuje dane wewnętrzne w kontekście funkcjonowania przedsiębiorstwa; omawia skutki ujawnienia poszczególnych kategorii danych; wyjaśnia, na czym polega przypisywanie poziomów poufności danych w przedsiębiorstwie; identyfikuje dane krytyczne dla ciągłości działania przedsiębiorstwa; reaguje na zidentyfikowane zagrożenia, zwracając uwagę współpracownikom na konieczność właściwego postępowania z danymi	Test teoretyczny z wynikiem generowanym automatycznie
4.2. Stosuje zasady bezpiecznego przetwarzania i przechowywania danych	Wyjaśnia, dlaczego powinno przetwarzać się tylko dane niezbędne; analizuje skutki nieuzasadnionego kopiowania danych; rozpoznaje ryzyko przechowywania danych na przenośnych nośnikach pamięci oraz lokalnych dyskach; stosuje szyfrowanie plików; korzysta z bezpiecznych platform transferu danych; reaguje na sytuacje nieprawidłowego przetwarzania lub przechowywania danych w środowisku pracy	Test teoretyczny z wynikiem generowanym automatycznie
4.3. Zapobiega wyciekom danych	Identyfikuje sytuacje mogące prowadzić do wycieku danych; rozpoznaje ryzyko korzystania z prywatnych urządzeń w celach służbowych; stosuje zasadę czystego biurka oraz blokowania komputera; zgłasza podejrzenie wycieku danych do przełożonego i współpracowników; zabezpiecza hasła oraz dane uwierzytelniające przed widocznością; wspiera współpracowników w stosowaniu zasad zapobiegających wyciekom danych	Test teoretyczny z wynikiem generowanym automatycznie Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
4.4. Postępuje zgodnie z zasadą odpowiedzialności i zgodności z przepisami o ochronie danych	Rozróżnia zakres odpowiedzialności pracownika i pracodawcy w obszarze ochrony danych; wyjaśnia konsekwencje prawne naruszeń przepisów w obszarze ochrony danych; rozpoznaje przypadki nieautoryzowanego dostępu do danych; stosuje zasady obiegu i przetwarzania dokumentów; wspiera innych pracowników w bezpiecznych praktykach dotyczących przetwarzania i przechowywania danych	Test teoretyczny z wynikiem generowanym automatycznie

Cel biznesowy

Usługa ogranicza ryzyko wycieku danych handlowych, osobowych i finansowych oraz kar wynikających z naruszenia przepisów o ochronie danych. Pracownik, który wie, które dane są krytyczne, szyfruje pliki przed wysłaniem i nie kopiuje danych na prywatne nośniki, eliminuje najczęstszą przyczynę wycieków w małych firmach – nieświadome działanie użytkownika. Szkolenie porządkuje też obieg dokumentów i skraca czas reakcji na podejrzenie wycieku.

Efekt usługi

Uczestnik bezpiecznie przetwarza, przechowuje i udostępnia dane: rozróżnia kategorie danych i przypisuje im poziomy poufności, stosuje zasadę przetwarzania wyłącznie danych niezbędnych, szyfruje pliki i korzysta z bezpiecznych kanałów transferu, rozpoznaje sytuacje mogące prowadzić do wycieku oraz zna zakres odpowiedzialności pracownika i pracodawcy.

Metoda potwierdzenia osiągnięcia efektu usługi

Efekty uczenia się osiągane są metodą warsztatową opartą na analizie przypadków i ćwiczeniach wykonywanych samodzielnie przez uczestników na materiale zbliżonym do realnej korespondencji służbowej. Osiągnięcie efektów potwierdza test wiedzy w formie elektronicznej – 30 pytań jednokrotnego wyboru, w tym pytania oparte na przypadkach, z progiem zaliczenia 70% – przeprowadzany w narzędziu generującym wynik automatycznie. Każde pytanie przypisane jest do kryteriów weryfikacji konkretnego efektu uczenia się, dzięki czemu wynik testu wskazuje, które efekty uczestnik osiągnął.

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

Szkolenie dwudniowe, 16 godzin zegarowych (2 dni po 8 godzin), realizowane zdalnie w czasie rzeczywistym. Zajęcia prowadzone są metodą warsztatową z ćwiczeniami wykonywanymi przez uczestników na własnym stanowisku pracy. Szkolenie nie wymaga wiedzy informatycznej. Grupa liczy od 2 do 15 osób.

DZIEŃ 1, SESJA 1 – Rodzaje danych i poziomy poufności (4 godziny) Rodzaje danych w przedsiębiorstwie: dane osobowe, finansowe, wewnętrzne. Skutki ujawnienia poszczególnych kategorii. Przypisywanie poziomów poufności – na czym polega i kto o nim decyduje. Dane krytyczne dla ciągłości działania przedsiębiorstwa. Warsztat: inwentaryzacja danych przetwarzanych na własnym stanowisku wraz z przypisaniem poziomów poufności.

DZIEŃ 1, SESJA 2 – Przetwarzanie i przechowywanie danych (4 godziny) Zasada przetwarzania wyłącznie danych niezbędnych. Skutki nieuzasadnionego kopiowania danych. Ryzyko przechowywania danych na przenośnych nośnikach pamięci i lokalnych dyskach. Warsztat praktyczny: szyfrowanie plików oraz korzystanie z bezpiecznych platform transferu danych.

DZIEŃ 2, SESJA 3 – Zapobieganie wyciekom danych (4 godziny) Sytuacje prowadzące do wycieku danych, ryzyko korzystania z urządzeń prywatnych w celach służbowych, zasada czystego biurka i blokowania komputera, zabezpieczanie haseł i danych uwierzytliwiających przed widocznością. Ścieżka zgłoszenia podejrzenia wycieku do przełożonego. Zadanie decyzyjne: pięć sytuacji ryzyka na własnym stanowisku i środki zaradcze.

DZIEŃ 2, SESJA 4 – Odpowiedzialność i zgodność (4 godziny wraz z walidacją) Zakres odpowiedzialności pracownika i pracodawcy w obszarze ochrony danych, konsekwencje prawne naruszeń, rozpoznawanie przypadków nieautoryzowanego dostępu, zasady obiegu i przetwarzania dokumentów.

ROZGRANICZENIE ZAKRESU Blok nr 4 obejmuje zasady postępowania z danymi: ich klasyfikację, przetwarzanie, przechowywanie, udostępnianie i zapobieganie wyciekom. Rozpoznawanie oszustw komputerowych stanowi odrębny blok nr 1 Rekomendacji RPK, cyberhigiena stanowiska pracy – odrębny blok nr 2, techniki manipulacji psychologicznej – odrębny blok nr 3, a postępowanie po stwierdzeniu incydentu, zabezpieczanie dowodów i zgłoszenie do CSIRT – odrębny blok nr 5. Żaden z tych zakresów nie wchodzi w zakres niniejszej usługi.

WALIDACJA EFEKTÓW UCZENIA SIĘ (30 minut, drugi dzień) Walidacja prowadzona jest metodą testu teoretycznego z wynikiem generowanym automatycznie. Test obejmuje 30 pytań jednokrotnego wyboru, w tym pytania oparte na przypadkach, i sprawdza wszystkie cztery efekty uczenia się zgodnie z przypisanymi im kryteriami weryfikacji. Test przeprowadzany jest w narzędziu elektronicznym generującym wynik automatycznie, bez udziału osoby oceniającej, co zapewnia rozdzielenie procesu kształcenia od procesu walidacji. Za organizację walidacji i dokumentowanie wyników odpowiada osoba walidująca wskazana w karcie usługi, niebędąca trenerem prowadzącym zajęcia. Uczestnik, który uzyska minimum 70% punktów, otrzymuje zaświadczenie ukończenia szkolenia zawierające opis efektów uczenia się, kryteria ich weryfikacji oraz zastosowane metody walidacji.

Harmonogram

Liczba pozycji harmonogramu: 11

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 11 Rodzaje danych w przedsiębiorstwie i poziomy poufności – warsztat inwentaryzacji i danych stanowiska	Zajęcia	Daniel Kacprowicz	12-01-2027	09:00	11:00	02:00
2 z 11 -	Przerwa	-	12-01-2027	11:00	11:15	00:15
3 z 11 Zasada minimalizacji danych, ryzyko nośników przenośnych, szyfrowanie plików i bezpieczne platformy transferu	Zajęcia	Daniel Kacprowicz	12-01-2027	11:15	13:15	02:00
4 z 11 -	Przerwa	-	12-01-2027	13:15	14:15	01:00
5 z 11 Warsztat praktyczny: szyfrowanie plików i korzystanie z bezpiecznych platform transferu danych	Zajęcia	Daniel Kacprowicz	12-01-2027	14:15	17:00	02:45
6 z 11 Zapobieganie wyciekom danych: sytuacje ryzyka, urządzenia prywatne, czyste biurko, zabezpieczanie haseł	Zajęcia	Daniel Kacprowicz	13-01-2027	09:00	11:00	02:00
7 z 11 -	Przerwa	-	13-01-2027	11:00	11:15	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
8 z 11 Zadanie decyzyjne: pięć sytuacji ryzyka wycieku na własnym stanowisku i środki zaradcze	Zajęcia	Daniel Kacprowicz	13-01-2027	11:15	13:15	02:00
9 z 11 -	Przerwa	-	13-01-2027	13:15	14:15	01:00
10 z 11 Odpowiedzialność pracownika i pracodawcy, konsekwencje prawne naruszeń, zasady obiegu dokumentów	Zajęcia	Daniel Kacprowicz	13-01-2027	14:15	16:30	02:15
11 z 11 -	Walidacja	-	13-01-2027	16:30	17:00	00:30

Podsumowanie

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

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 080,00 PLN

Koszt przypadający na 1 uczestnika netto	2 080,00 PLN
Koszt osobogodziny brutto	130,00 PLN
Koszt osobogodziny netto	130,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	16:00

Prowadzący

Liczba prowadzących: 1



1 z 1

Daniel Kacprowicz

Prezes Zarządu AD-TRADE Sp. z o.o., właściciel marki szkoleniowej szkolimy24.com. Trener z udokumentowanym doświadczeniem ponad 290 godzin przeprowadzonych szkoleń z zakresu kompetencji cyfrowych, obsługi komputera i internetu oraz cyberbezpieczeństwa (potwierdzone referencjami: ODZ BHP Ekspert, MOPR Włocławek, MAXDOM, Klub Senior+). Prowadzi szkolenia z praktycznego zastosowania narzędzi sztucznej inteligencji dla pracowników administracji publicznej, jednostek pomocy społecznej, placówek oświatowych oraz firm sektora MŚP – m.in. szkolenie z cyberbezpieczeństwa, ochrony danych osobowych i narzędzi AI dla 52 pracowników Miejskiego Ośrodka Pomocy Rodzinie we Włocławku oraz szkolenia z AI i narzędzi wizualnych dla placówek oświatowych. Specjalizacja: wdrażanie narzędzi generatywnej sztucznej inteligencji (ChatGPT, Microsoft Copilot, Google Gemini) w pracy biurowej i administracyjnej, prompt engineering, bezpieczeństwo danych w środowisku AI oraz automatyzacja powtarzalnych zadań biurowych.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy uczestnik otrzymuje pakiet materiałów przygotowanych przez szkolimy24.com: skrypt PDF „Bezpieczne przetwarzanie i udostępnianie danych”, szablon inwentaryzacji danych stanowiska z poziomami poufności, instrukcję szyfrowania plików, listę bezpiecznych kanałów transferu danych, kartę zasad czystego biurka, zestaw sytuacji ryzyka wycieku do zadania decyzyjnego, schemat obiegu dokumentów oraz nagrania czterech sesji. Materiały przekazywane są w formie cyfrowej i pozostają dostępne przez 12 miesięcy.

Warunki techniczne

Usługa realizowana zdalnie w czasie rzeczywistym na platformie Zoom — spotkanie z rejestracją uczestników i funkcją nagrywania.

Minimalne wymagania sprzętowe: komputer klasy PC lub Mac z procesorem dwurdzeniowym 2 GHz i pamięcią 4 GB RAM, kamera internetowa, mikrofon oraz głośniki lub zestaw słuchawkowy.

Minimalne wymagania dotyczące parametrów łącza sieciowego: łącze internetowe o przepustowości minimum 5 Mb/s dla pobierania i 2 Mb/s dla wysyłania.

Niezbędne oprogramowanie: przeglądarka internetowa w aktualnej wersji (Google Chrome, Microsoft Edge lub Mozilla Firefox) albo aplikacja Zoom; pakiet biurowy oraz konto w narzędziu AI (ChatGPT, Microsoft Copilot lub Google Gemini) — wystarczające są konta w wersjach bezpłatnych.

Okres ważności linku: link do spotkania jest aktywny przez cały czas trwania usługi i zostaje przesłany uczestnikom pocztą elektroniczną najpóźniej 24 godziny przed rozpoczęciem zajęć.

Sposób weryfikacji obecności: rejestr wejść i wyjść uczestników generowany przez platformę, weryfikacja tożsamości na podstawie włączonej kamery podczas zajęć oraz podczas walidacji efektów uczenia się.

Przebieg usługi jest rejestrowany (nagrywany) w celu udokumentowania jej realizacji zgodnie z wymogami obowiązującymi dla usług zdalnych w Bazie Usług Rozwojowych.

Kontakt



Daniel Kacprowicz

E-mail biuro@szkolimy24.com

Telefon (+48) 508 325 677