Możliwość dofinansowania

AD-TRADE SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

Brak ocen dla tego dostawcy

Stosowanie zasad cyberhigieny w codziennej pracy z narzędziami cyfrowymi i urządzeniami końcowymi w MŚP

Numer usługi 2026/09/07/205802/3794081

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

Usługa szkoleniowa
zdalna w czasie rzeczywistym
Zajęcia grupowe
16:00 h
08.12.2026 do 09.12.2026

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	01-12-2026
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 stosowania zasad cyberhigieny: bezpiecznego zarządzania hasłami i dostępem, utrzymywania urządzeń i oprogramowania w stanie zmniejszającym ryzyko, bezpiecznego korzystania z sieci oraz tworzenia kopii zapasowych. Uczestnik tworzy hasła spełniające zasady bezpieczeństwa, korzysta z menedżera haseł i uwierzytelniania wieloskładnikowego, ogranicza uprawnienia aplikacji, rozpoznaje podejrzane sieci publiczne i wskazuje dane wymagające kopii zapasowej.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
2.1. Rozumie zasady cyberhigieny	Definiuje pojęcie cyberhigieny oraz jej rolę w bezpieczeństwie organizacji; wymienia podstawowe zasady bezpiecznego korzystania z narzędzi cyfrowych; omawia rolę użytkownika w systemie cyberbezpieczeństwa; wskazuje najczęstsze błędy użytkowników prowadzące do incydentów; wyjaśnia rolę użytkownika jako pierwszej linii obrony; reaguje na zaobserwowane działania współpracowników zwiększające ryzyko incydentu cyberbezpieczeństwa	Test teoretyczny z wynikiem generowanym automatycznie
2.2. Stosuje zasady bezpiecznego zarządzania hasłami i dostępem	Tworzy hasła spełniające zasady bezpieczeństwa; rozróżnia hasła silne i słabe; stosuje zasadę unikalności haseł; wyjaśnia rolę menedżerów haseł; omawia korzyści związane z wykorzystywaniem uwierzytelniania wieloskładnikowego (MFA); reaguje na zaobserwowane działania współpracowników wskazujące na naruszenia zasad bezpiecznego zarządzania hasłami w środowisku pracy	Test teoretyczny z wynikiem generowanym automatycznie
2.3. Stosuje zasady bezpieczeństwa urządzeń i oprogramowania	Wyjaśnia znaczenie aktualizacji systemów i aplikacji; stosuje blokadę ekranu i zabezpieczenia biometryczne; rozpoznaje ryzyko instalacji nieznanych aplikacji; wskazuje skutki braku aktualizacji dla cyberbezpieczeństwa; weryfikuje i ogranicza uprawnienia aplikacji do niezbędnego zakresu; reaguje na zaobserwowane działania współpracowników wskazujące na nieprawidłowe korzystanie z urządzeń i oprogramowania w środowisku pracy	Test teoretyczny z wynikiem generowanym automatycznie Test teoretyczny z wynikiem generowanym automatycznie Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
2.4. Stosuje zasady bezpiecznego korzystania z sieci	Wskazuje ryzyka związane z korzystaniem z publicznych sieci WiFi; odróżnia sieć publiczną od prywatnej; wskazuje korzyści stosowania VPN; rozpoznaje sytuacje wymagające unikania korzystania z publicznych sieci WiFi; rozpoznaje podejrzane sieci publiczne WiFi; informuje współpracowników o zidentyfikowanych zagrożeniach związanych z korzystaniem z publicznych sieci Wi-Fi	Test teoretyczny z wynikiem generowanym automatycznie
2.5. Stosuje podstawowe zasady tworzenia kopii zapasowych	Definiuje pojęcie kopii zapasowej; wyjaśnia cel tworzenia kopii zapasowej; wskazuje dane wymagające kopii zapasowej z punktu widzenia funkcjonowania przedsiębiorstwa; omawia skutki braku kopii zapasowej; wyjaśnia różnicę pomiędzy kopią zapasową lokalną i chmurową; reaguje na sytuacje braku kopii zapasowej lub ryzyka utraty danych w środowisku pracy	Test teoretyczny z wynikiem generowanym automatycznie

Cel biznesowy

Usługa ogranicza ryzyko incydentów wynikających z zachowań użytkowników — przejęcia konta wskutek słabego lub powtórzonego hasła, infekcji urządzenia po instalacji nieznanej aplikacji, przechwycenia danych w otwartej sieci oraz utraty danych przy braku kopii zapasowej. Zmniejsza liczbę zgłoszeń do obsługi informatycznej i skraca czas przywrócenia pracy po awarii lub utracie danych.

Efekt usługi

Uczestnik stosuje zasady cyberhigieny w codziennej pracy: tworzy i utrzymuje hasła spełniające zasady bezpieczeństwa, korzysta z menedżera haseł i uwierzytelniania wieloskładnikowego, utrzymuje aktualne oprogramowanie i ogranicza uprawnienia aplikacji, rozpoznaje podejrzane sieci publiczne oraz wskazuje dane wymagające kopii zapasowej i właściwy jej rodzaj.

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 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 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 — Cyberhigiena: pojęcie i rola użytkownika (4 godziny) Cyberhigiena: pojęcie i rola w bezpieczeństwie organizacji. Podstawowe zasady bezpiecznego korzystania z narzędzi cyfrowych. Rola użytkownika w systemie cyberbezpieczeństwa i jako pierwszej linii obrony. Najczęstsze błędy użytkowników prowadzące do incydentów. Warsztat: przegląd cyberhigieny własnego stanowiska pracy na arkuszu startowym.

DZIEŃ 1, SESJA 2 — Hasła, dostęp i uwierzytelnianie wieloskładnikowe (4 godziny) Konstrukcja hasła spełniającego zasady bezpieczeństwa, hasła silne a słabe, zasada unikalności. Menedżery haseł — rola i zasady użycia. Uwierzytelnianie wieloskładnikowe (MFA): korzyści i typowe warianty. Zadanie praktyczne w środowisku symulowanym: utworzenie hasła, wpis w menedżerze, konfiguracja MFA.

DZIEŃ 2, SESJA 3 — Urządzenia i oprogramowanie (4 godziny) Znaczenie aktualizacji systemów i aplikacji oraz skutki ich braku. Blokada ekranu i zabezpieczenia biometryczne. Ryzyko instalacji nieznanych aplikacji. Warsztat: weryfikacja i ograniczenie uprawnień aplikacji do niezbędnego zakresu na urządzeniu służbowym.

DZIEŃ 2, SESJA 4 — Sieci i kopie zapasowe (4 godziny wraz z walidacją) Ryzyka publicznych sieci WiFi, odróżnienie sieci publicznej od prywatnej, rozpoznawanie podejrzanych sieci, korzyści i granice VPN. Kopie zapasowe: pojęcie i cel, dane wymagające kopii z punktu widzenia funkcjonowania przedsiębiorstwa, skutki braku kopii, kopia lokalna a chmurowa. Zadanie praktyczne: plan kopii zapasowych dla własnego stanowiska.

ROZGRANICZENIE ZAKRESU Blok nr 2 obejmuje nawyki i ustawienia po stronie użytkownika: hasła, dostęp, urządzenia, oprogramowanie, sieci i kopie zapasowe. Rozpoznawanie oszustw komputerowych i analiza ich scenariuszy stanowią odrębny blok nr 1 Rekomendacji RPK. Techniki manipulacji psychologicznej stanowią odrębny blok nr 3. Klasyfikacja danych, szyfrowanie plików, bezpieczne platformy transferu i zapobieganie wyciekom stanowią odrębny blok nr 4 — niniejsza usługa dotyczy kopii zapasowej jako środka ciągłości działania, nie zasad przetwarzania i udostępniania danych. Postępowanie po wykryciu incydentu stanowi 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 pięć efektów 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: 12

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 12 Cyberhigiena: pojęcie, rola użytkownika jako pierwszej linii obrony, najczęstsze błędy prowadzące do incydentów	Zajęcia	Daniel Kacprowicz	08-12-2026	09:00	11:00	02:00
2 z 12 -	Przerwa	-	08-12-2026	11:00	11:15	00:15
3 z 12 Hasła i dostęp: konstrukcja hasła, menedżer haseł, uwierzytelnianie wieloskładnikowe — zadanie praktyczne	Zajęcia	Daniel Kacprowicz	08-12-2026	11:15	13:15	02:00
4 z 12 -	Przerwa	-	08-12-2026	13:15	14:15	01:00
5 z 12 Urządzenia i oprogramowanie: aktualizacje, blokada ekranu, uprawnienia aplikacji — warsztat na urządzeniu służbowym	Zajęcia	Daniel Kacprowicz	08-12-2026	14:15	17:00	02:45

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
6 z 12 Sieci: publiczne WiFi, rozpoznawanie podejrzanych sieci, VPN — zadanie decyzyjne	Zajęcia	Daniel Kacprowicz	09-12-2026	09:00	11:00	02:00
7 z 12 -	Przerwa	-	09-12-2026	11:00	11:15	00:15
8 z 12 Kopie zapasowe: dane wymagające kopii, kopia lokalna a chmurowa, plan kopii dla stanowiska pracy	Zajęcia	Daniel Kacprowicz	09-12-2026	11:15	13:15	02:00
9 z 12 -	Przerwa	-	09-12-2026	13:15	13:45	00:30
10 z 12 -	Przerwa	-	09-12-2026	13:45	14:15	00:30
11 z 12 Warsztat podsumowujący: przegląd cyberhigieny stanowiska pracy i plan wdrożenia zmian	Zajęcia	Daniel Kacprowicz	09-12-2026	14:15	16:30	02:15
12 z 12 -	Walidacja	-	09-12-2026	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

Rodzaj godzin	Liczba godzin
Suma godzin dydaktycznych bez przerw	18:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 080,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
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 „Cyberhigiena w codziennej pracy", arkusz przeglądu cyberhigieny stanowiska pracy, instrukcję konfiguracji menedżera haseł i uwierzytelniania wieloskładnikowego, szablon planu kopii zapasowych, listę kontrolną uprawnień aplikacji, zestaw sytuacji sieciowych do zadania decyzyjnego 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