Możliwość dofinansowania

Cyberbezpieczeństwo dla pracowników biurowych i administracji – usługa szkoleniowa

Numer usługi 2026/03/31/161638/3450975

4 428,00 PLN brutto
3 600,00 PLN netto
147,60 PLN brutto/h
120,00 PLN netto/h
261,33 PLN cena rynkowa

KORYCKI & GRACZYK CONSULTING GROUP SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

4,9 / 5

667 ocen

Usługa szkoleniowa
zdalna w czasie rzeczywistym
30:00 h
06.07.2026 do 08.07.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikatory projektów	Kierunek - Rozwój, Nowy start w Małopolsce z EURESEM, Małopolski Pociąg do kariery, Zachodniopomorskie Bony Szkoleniowe
Grupa docelowa usługi	• Pracownicy biurowi, administracja, sekretariaty, recepcje, kancelarie, działy kadr, księgowości, obsługi klienta, back-office itp. • Pracownicy jednostek administracji publicznej oraz firm prywatnych przetwarzający dane i informacje (w tym dane osobowe). • Osoby przygotowujące się do pracy na stanowiskach administracyjnych. • Uczestnicy projektów: **Małopolski Pociąg do Kariery**, **Nowy Start w Małopolsce (EURES)**, **Kierunek Rozwój**. • Usługa rozwojowa adresowana również dla Uczestników projektu **Zachodniopomorskie Bony Szkoleniowe.**
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	5
Data zakończenia rekrutacji	02-07-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	30
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Usługa pn. „Cyberbezpieczeństwo dla pracowników biurowych i administracji – usługa szkoleniowa” przygotowuje uczestników do bezpiecznego wykonywania codziennych czynności służbowych w środowisku cyfrowym poprzez nabycie i uaktualnienie wiedzy oraz umiejętności z zakresu cyberbezpieczeństwa, ochrony danych i reagowania na incydenty, bezpośrednio związanych z typowymi zadaniami pracowników biurowych i administracji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Definiuje podstawowe pojęcia z zakresu cyberbezpieczeństwa (m.in. złośliwe oprogramowanie, phishing, ransomware, socjotechnika, inżynieria społeczna, incydent bezpieczeństwa)	Rozróżnia pojęcia na podstawie opisanych sytuacji	Test teoretyczny z wynikiem generowanym automatycznie
	Podaje co najmniej jeden przykład praktyczny dla każdego z pojęć	Wywiad swobodny
	Wskazuje kluczowe cechy każdego pojęcia	Wywiad swobodny
Rozpoznaje główne grupy zagrożeń typowych dla stanowisk biurowo-administracyjnych	Rozróżnia zagrożenia „ludzkie” od technicznych i organizacyjnych	Wywiad swobodny
	Wymienia główne grupy zagrożeń	Wywiad swobodny
	Przyporządkowuje przykłady do grup zagrożeń	Wywiad swobodny
Stosuje zasady tworzenia i przechowywania silnych haseł oraz wykorzystuje mechanizmy uwierzytelniania wieloskładnikowego	Rozróżnia hasło silne od słabego	Test teoretyczny z wynikiem generowanym automatycznie
	Charakteryzuje zasady bezpiecznego przechowywania haseł	Wywiad swobodny
	Reaguje poprawnie na opisane scenki	Test teoretyczny z wynikiem generowanym automatycznie
Identyfikuje sytuacje, w których wymagana jest szczególna ostrożność	Rozpoznaje sytuacje ryzykowne w opisanych scenkach	Test teoretyczny z wynikiem generowanym automatycznie
	Rozróżnia sytuacje standardowe od „czerwonych flag”	Test teoretyczny z wynikiem generowanym automatycznie
	Wymienia przykłady sytuacji wymagających szczególnej ostrożności	Wywiad swobodny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wyjaśnia podstawowe zasady ochrony danych osobowych oraz informacji poufnych obowiązujące w administracji/publicznym lub prywatnym pracodawcy	Wyjaśnia, czym są dane osobowe i informacje poufne	Test teoretyczny z wynikiem generowanym automatycznie
	Wskazuje podstawowe zasady ochrony danych i informacji	Test teoretyczny z wynikiem generowanym automatycznie
Wyróżnia dobre praktyki w obszarze haseł, logowania, pracy zdalnej, nośników danych, korzystania z Wi-Fi i urządzeń mobilnych	Rozróżnia dobre i złe praktyki na przykładach	Test teoretyczny z wynikiem generowanym automatycznie
	Charakteryzuje dobre praktyki w każdym z obszarów	Wywiad swobodny
	Uzasadnia spójność dobrych praktyk	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

Dzień 1 — Podstawy cyberbezpieczeństwa w pracy biurowej, bezpieczna praca na komputerze i w sieci

(10 godzin dydaktycznych; 8:00–16:45, 2 przerwy po 15 min, 1 przerwa obiadowa 45 min)

8:00–8:45 – Wprowadzenie do szkolenia

Cel i zakres szkolenia, kształcenie zawodowe, program 3-dniowy, zasady pracy on-line i przerw, kontrakt grupowy, poufność przykładów z pracy uczestników.

8:45–9:30 – Podstawy cyberbezpieczeństwa

Definicja „dla ludzi”, filary (poufność, integralność, dostępność), dlaczego dotyczy każdego pracownika biurowego, konsekwencje incydentów dla organizacji i pracownika.

09:30–09:45 – Przerwa kawowa

09:45–11:15 – Zasoby i zagrożenia

Identyfikacja zasobów (dane osobowe, dokumenty, loginy i dostępy do systemów), najczęstsze zagrożenia (phishing, smishing, vishing, fałszywe faktury, „pilne płatności”), praca na case studies.

11:15–11:30 – Przerwa kawowa

11:30–13:00 – Pojęcia dla nieinformatyków

Wyjaśnienie kluczowych pojęć (malware, ransomware, exploit, podatność, incydent), łączenie pojęć z realnymi sytuacjami, mini-quiz, podsumowanie.

13:00–13:45 – Przerwa obiadowa

13:45–14:30 – „Moje ryzyka w pracy”

Indywidualna mapa ryzyk związanych z wykonywanymi zadaniami (poczta, dokumenty, systemy), praca w parach/podgrupach, lista najważniejszych ryzyk typowego pracownika biurowego.

14:30–15:15 – Hasła, loginy i uprawnienia

Rola haseł i loginów w używanych systemach, najczęstsze błędy (słabe hasła, powtarzanie, zapisywanie na kartkach), poziomy uprawnień, krótkie omówienie polityki haseł w organizacji.

15:15–16:00 – Metody ustalania silnych haseł – ćwiczenia

Zasady tworzenia silnych, używalnych haseł, 2–3 proste metody (np. hasło-zdanie), najczęstsze ataki na hasła, ćwiczenia na bezpiecznych przykładach.

16:00–16:45 – Uwierzytelnianie wieloskładnikowe (MFA/2FA) w praktyce

Na czym polega MFA, przebieg logowania krok po kroku, najczęstsze błędy użytkowników (bezrefleksyjne potwierdzanie, podawanie kodów), krótkie case studies „klikam czy zgłaszam?”.

Dzień 2 — Bezpieczna praca na komputerze i w sieci (część zaawansowana)

(10 godzin dydaktycznych; 8:00–16:45, 2 przerwy po 15 min, 1 przerwa obiadowa 45 min)

8:00–9:30 – Ochrona urządzenia: programy antywirusowe i aktualizacje

Rola antywirusa/antymalware, znaczenie aktualizacji systemu i oprogramowania, podstawowe sprawdzenie działania ochrony, praktyczne zalecenia dla pracownika (co wolno, czego nie robić samodzielnie, kiedy zgłosić się do IT).

9:30–9:45 – Przerwa kawowa

9:45–11:15 – Szyfrowanie dokumentów i plików + bezpieczne wysyłanie

Szyfrowanie „dla użytkownika”, szyfrowane dokumenty/archiwa, zasady wysyłania zabezpieczonych dokumentów (osobny kanał dla hasła, weryfikacja adresata, minimalizacja danych), wypracowanie prostej procedury bezpiecznej wysyłki.

11:15–11:30 – Przerwa kawowa

11:30–13:00 – Kopie zapasowe (backup) i bezpieczne przechowywanie danych

Czym jest backup, jak organizacje go realizują (dyski sieciowe, chmura firmowa – w zarysie), rola pracownika (gdzie zapisywać pliki, czego unikać), minicase „ransomware i brak kopii”, checklista zapisywania plików.

13:00–13:45 – Przerwa obiadowa

13:45–14:30 – Bezpieczne korzystanie z przeglądarki

Tryb prywatny/incognito i jego ograniczenia, zapamiętywanie haseł w przeglądarce, ciasteczka i autologowanie, dobre nawyki pracy z przeglądarką w biurze i w domu.

14:30–15:15 – VPN i bezpieczna praca zdalna

VPN z perspektywy użytkownika, kiedy jest konieczny (dostęp do zasobów wewnętrznych, praca spoza biura), praca w publicznych Wi-Fi, ćwiczenie decyzyjne „loguję się czy czekam?".

15:15–16:00 – Objawy incydentu: jak poznać, że „coś jest nie tak"

Typowe objawy problemów na komputerze/konto (dziwne okna, spowolnienie, dziwne wiadomości), co zrobić i czego nie robić, krótkie case studies.

16:00–16:45 – Jak zgłaszać incydenty w praktyce

Definicja incydentu z perspektywy pracownika, do kogo zgłaszamy (IT, przełożony, IOD), jakie informacje przekazać, przykładowy formularz zgłoszenia incydentu i krótkie ćwiczenie.

Dzień 3 — Ochrona danych i informacji, socjotechnika, phishing i walidacja

(10 godzin dydaktycznych; 8:00–16:45, 2 przerwy po 15 min, 1 przerwa obiadowa 45 min)

8:00–9:30 – RODO z perspektywy pracownika biurowego

Słowniczek podstawowych pojęć (administrator, podmiot danych, przetwarzanie, naruszenie), zasada minimalizacji danych („need to know") w codziennych zadaniach, przykłady naruszeń z życia biura.

9:30–9:45 – Przerwa kawowa

9:45–10:30 – Typowe błędy w ochronie danych – case studies

Analiza kilku naruszeń (zły adresat, pozostawione wydruki, przesyłanie na prywatne konto), lista „TOP błędów pracownika biurowego i jak ich unikać".

10:30–11:15 – Deepfake i inne rozwiązania AI budujące dezinformację

Przykłady deepfake'ów i zniekształconych zdjęć (prosty test rozpoznawania), omówienie, jak generatywna AI ułatwia tworzenie fałszywych treści (maile, dokumenty) i jakie to ma znaczenie dla pracownika biurowego.

11:15–11:30 – Przerwa kawowa

11:30–12:15 – Praca z dokumentami i systemami w praktyce

Zasady udostępniania dokumentów osobom trzecim, zasady archiwizacji i niszczenia dokumentów (papierowych i elektronicznych), dostęp do systemów z danymi (co wolno, czego nie wolno).

12:15–13:00 – Inżynieria społeczna (wprowadzenie)

Czym jest cyberatak i dlaczego inżynieria społeczna jest tak skuteczna, definicja socjotechniki, podstawy socjologiczne i psychologiczne (autorytet, pilność, lęk, chęć pomocy).

13:00–13:45 – Przerwa obiadowa

13:45–14:30 – Socjotechnika w praktyce

Metody wywierania wpływu na pracowników, typowe scenariusze z biura/urzędu (telefon „z banku/prezesa/IT"), krótkie scenki i omówienie reakcji.

14:30–15:15 – Phishing w praktyce

Quiz na przykładach maili/SMS-ów, klasyfikacja wiadomości (bezpieczna/podejrzana/niebezpieczna), omówienie wyników i checklisty oceny podejrzanej wiadomości.

15:15–16:00 – Walidacja – test teoretyczny z wynikiem generowanym automatycznie

Test on-line (Formularz Google) obejmujący treści szkolenia, automatyczny wynik, próg zaliczenia 80%.

16:00–16:45 – Walidacja – wywiad swobodny z walidatorem

Indywidualna rozmowa (kamera włączona) dotycząca roli zawodowej uczestnika, zrozumienia kluczowych zagadnień, wykonanych ćwiczeń i planowanych działań wdrożeniowych; informacja zwrotna i wynik walidacji.

1) Godziny i forma

Szkolenie odbywa się w godzinach dydaktycznych (1 godz. = 45 minut), łącznie **30 godzin dydaktycznych**. Usługa realizowana jest zdalnie, w czasie rzeczywistym, na platformie **Google Meet**. Przerwy (dwie po 15 minut i jedna 45-minutowa w każdym dniu) nie są wliczane do czasu szkolenia. Grupy: **1–5 osób**.

2) Metoda prowadzenia

Zajęcia prowadzone są metodami **interaktywnymi i aktywizującymi**: krótkie wprowadzenia trenera, studia przypadków, ćwiczenia indywidualne, quizy on-line, dyskusje moderowane, praca na checklistach i prostych procedurach.

3) Grupa docelowa. Usługa skierowana jest do:

- pracowników biurowych, administracji, sekretariatów, recepcji, kancelarii, działów kadr, księgowości, obsługi klienta, back-office itp.,
- pracowników jednostek administracji publicznej oraz firm prywatnych przetwarzających dane i informacje (w tym dane osobowe),
- osób przygotowujących się do pracy na stanowiskach administracyjnych.

Usługa przeznaczona jest również dla Uczestników projektów: **Małopolski Pociąg do Kariery**, **Nowy Start w Małopolsce (EURES)**, **Kierunek Rozwój**, a także adresowana do Uczestników projektu **Zachodniopomorskie Bony Szkoleniowe**.

4) Cel edukacyjny. Usługa pn. „Cyberbezpieczeństwo dla pracowników biurowych i administracji – usługa szkoleniowa" przygotowuje uczestników do bezpiecznego wykonywania codziennych czynności służbowych w środowisku cyfrowym poprzez nabycie i uaktualnienie wiedzy oraz umiejętności z zakresu cyberbezpieczeństwa, ochrony danych i reagowania na incydenty, bezpośrednio związanych z typowymi zadaniami pracowników biurowych i administracji.

5) Walidacja – kryteria ogólne

Uczestnik otrzyma zaświadczenie po spełnieniu dwóch warunków:

- frekwencja co najmniej **80% czasu szkolenia** (bez przerw) oraz
- wynik walidacji na poziomie minimum **80%** (test + wywiad).

Ocenie podlega w szczególności: merytoryczna poprawność odpowiedzi, zwięzłość i klarowność wypowiedzi oraz dopasowanie przykładów i rozwiązań do specyfiki pracy uczestnika.

6) Charakter usługi (VAT)

Szkolenie stanowi usługę **kształcenia zawodowego** w rozumieniu art. 43 ust. 1 pkt 29 ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług, tj. nauczanie pozostające w bezpośrednim związku z branżą i zawodem pracowników biurowych i administracji oraz służące uzyskaniu lub uaktualnieniu wiedzy do celów zawodowych, zgodnie z definicją przyjętą w rozporządzeniu wykonawczym Rady UE nr 282/2011.

Harmonogram

Liczba pozycji harmonogramu: 33

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 33 Wprowadzenie do szkolenia – wideokonferencja	WOJCIECH GRACZYK	06-07-2026	08:00	08:45	00:45

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
2 z 33 Podstawy cyberbezpieczeństwa – wideokonferencja	WOJCIECH GRACZYK	06-07-2026	08:45	09:30	00:45
3 z 33 Przerwa kawowa	WOJCIECH GRACZYK	06-07-2026	09:30	09:45	00:15
4 z 33 Zasoby i zagrożenia – rozmowa na żywo	WOJCIECH GRACZYK	06-07-2026	09:45	11:15	01:30
5 z 33 Przerwa kawowa	WOJCIECH GRACZYK	06-07-2026	11:15	11:30	00:15
6 z 33 Pojęcia dla nieinformatyków – wideokonferencja	WOJCIECH GRACZYK	06-07-2026	11:30	13:00	01:30
7 z 33 Przerwa obiadowa	WOJCIECH GRACZYK	06-07-2026	13:00	13:45	00:45
8 z 33 „Moje ryzyka w pracy” – ćwiczenia	WOJCIECH GRACZYK	06-07-2026	13:45	14:30	00:45
9 z 33 Hasła, loginy i uprawnienia – wideokonferencja	WOJCIECH GRACZYK	06-07-2026	14:30	15:15	00:45
10 z 33 Metody ustalania silnych haseł – ćwiczenia	WOJCIECH GRACZYK	06-07-2026	15:15	16:00	00:45
11 z 33 Uwierzytelnianie wieloskładnikowe (MFA/2FA) w praktyce – współdzielenie ekranu	WOJCIECH GRACZYK	06-07-2026	16:00	16:45	00:45

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
12 z 33 Ochrona urządzenia: programy antywirusowe i aktualizacje – wideokonferencja	WOJCIECH GRACZYK	07-07-2026	08:00	09:30	01:30
13 z 33 Przerwa kawowa	WOJCIECH GRACZYK	07-07-2026	09:30	09:45	00:15
14 z 33 Szyfrowanie dokumentów i plików + bezpieczne wysyłanie – ćwiczenia	WOJCIECH GRACZYK	07-07-2026	09:45	11:15	01:30
15 z 33 Przerwa kawowa	WOJCIECH GRACZYK	07-07-2026	11:15	11:30	00:15
16 z 33 Kopie zapasowe (backup) i bezpieczne przechowywanie danych – współdzielenie ekranu	WOJCIECH GRACZYK	07-07-2026	11:30	13:00	01:30
17 z 33 Przerwa obiadowa	WOJCIECH GRACZYK	07-07-2026	13:00	13:45	00:45
18 z 33 Bezpieczne korzystanie z przeglądarki – wideokonferencja	WOJCIECH GRACZYK	07-07-2026	13:45	14:30	00:45
19 z 33 VPN i bezpieczna praca zdalna – współdzielenie ekranu	WOJCIECH GRACZYK	07-07-2026	14:30	15:15	00:45
20 z 33 Objawy incydentu: jak poznać, że „coś jest nie tak” – rozmowa na żywo	WOJCIECH GRACZYK	07-07-2026	15:15	16:00	00:45

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
21 z 33 Jak zgłaszać incydenty w praktyce – ćwiczenia	WOJCIECH GRACZYK	07-07-2026	16:00	16:45	00:45
22 z 33 RODO z perspektywy pracownika biurowego – wideokonferencja	WOJCIECH GRACZYK	08-07-2026	08:00	09:30	01:30
23 z 33 Przerwa kawowa	WOJCIECH GRACZYK	08-07-2026	09:30	09:45	00:15
24 z 33 Typowe błędy w ochronie danych – case studies – współdzielenie ekranu	WOJCIECH GRACZYK	08-07-2026	09:45	10:30	00:45
25 z 33 Deepfake i inne rozwiązania AI budujące dezinformację – współdzielenie ekranu	WOJCIECH GRACZYK	08-07-2026	10:30	11:15	00:45
26 z 33 Przerwa kawowa	WOJCIECH GRACZYK	08-07-2026	11:15	11:30	00:15
27 z 33 Praca z dokumentami i systemami w praktyce – rozmowa na żywo	WOJCIECH GRACZYK	08-07-2026	11:30	12:15	00:45
28 z 33 Inżynieria społeczna (wprowadzenie) – wideokonferencja	WOJCIECH GRACZYK	08-07-2026	12:15	13:00	00:45
29 z 33 Przerwa obiadowa	WOJCIECH GRACZYK	08-07-2026	13:00	13:45	00:45

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
30 z 33 Socjotechnika w praktyce – współdzielenie ekranu	WOJCIECH GRACZYK	08-07-2026	13:45	14:30	00:45
31 z 33 Phishing w praktyce – ćwiczenia	WOJCIECH GRACZYK	08-07-2026	14:30	15:15	00:45
32 z 33 Walidacja – test teoretyczny z wynikiem generowanym automatycznie	-	08-07-2026	15:15	16:00	00:45
33 z 33 Walidacja – wywiad swobodny z walidatorem	-	08-07-2026	16:00	16:45	00:45

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	4 428,00 PLN
Koszt przypadający na 1 uczestnika netto	3 600,00 PLN
Koszt osobogodziny brutto	147,60 PLN
Koszt osobogodziny netto	120,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

WOJCIECH GRACZYK

Wojciech Graczyk — ekspert ds. cyberbezpieczeństwa, bezpieczeństwa informacji oraz walidator, Prezes Zarządu KORYCKI & GRACZYK CONSULTING GROUP sp. z o.o. Specjalizuje się w projektowaniu i utrzymaniu systemów bezpieczeństwa cyfrowego w organizacjach szkoleniowych, łącząc perspektywę prawną, techniczną i trenerską. Posiada ponad 3000 udokumentowanych godzin prowadzenia szkoleń, w tym ponad 1000 godzin w obszarze bezpieczeństwa cyfrowego i higieny pracy w ostatnich pięciu latach, oraz doświadczenie w realizacji ponad 200 procesów walidacyjnych.

Od ponad dwóch lat odpowiada za wdrażanie i utrzymanie zgodności standardów świadczenia usług szkoleniowych ze szczególnym naciskiem na bezpieczeństwo informacji – przygotowuje i opiniuje umowy, tworzy regulacje i regulaminy, a także projektuje i doskonali procesy szkoleniowe end-to-end w sposób zapewniający ochronę danych oraz minimalizację ryzyk cybernetycznych.

Posiada trzy certyfikaty trenerskie potwierdzające kompetencje do prowadzenia szkoleń dla osób dorosłych.

Aktualnie studiuje na V roku prawa, co pozwala mu łączyć praktykę cyberbezpieczeństwa i bezpieczeństwa informacji z podejściem prawnym i compliance. Łączy perspektywę merytoryczną trenera z procesowym spojrzeniem na organizację oraz najwyższą starannością operacyjną, kładąc nacisk na zgodność z przepisami, transparentność oraz realny efekt i bezpieczeństwo po stronie klienta.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Prezentacja w formacie PDF oraz checklisty w formacie PDF.

Warunki uczestnictwa

- Podstawowa obsługa komputera i poczty elektronicznej.
- Brak wymogu specjalistycznej wiedzy IT – szkolenie jest projektowane dla „zwykłego użytkownika", ale w kontekście jego obowiązków zawodowych.
- Ukończony 18 rok życia

Informacje dodatkowe

1. Jeśli szkolenie będzie dofinansowane ze środków publicznych w **co najmniej 70%,** będzie **zwolnione przedmiotowo z podatku VAT** (podstawa prawna: par. 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* (t.j. Dz. U. z 2023 r. poz. 955 z późn. zm.)).
2. Zawarto **Umowę ramową numer RR.0716.275.2024 z WUP w Toruniu** dotycząca realizacji i rozliczania Usług z wykorzystaniem bonów elektronicznych w ramach **Projektu Kierunek – Rozwój**.
3. Uczestnik szkolenia otrzyma zaświadczenie o ukończeniu szkolenia dopiero po pozytywnym wyniku walidacji. Warunkiem otrzymania zaświadczenia o ukończeniu szkolenia jest **pozytywny wynik walidacji** oraz **frekwencja na minimalnym poziomie 80%**.
4. Zawarto umowę z Wojewódzkim Urzędem Pracy w Szczecinie na świadczenie usług rozwojowych z wykorzystaniem elektronicznych bonów szkoleniowych w ramach projektu Zachodniopomorskie Bony Szkoleniowe.

Warunki techniczne

1. **Platforma komunikacyjna** – Google Meet.

2. **Wymagania sprzętowe:**

- komputer z aktualnym systemem (Windows 10 lub nowszy / macOS 12 lub nowszy / aktualna dystrybucja Linux),
- aktualna przeglądarka (Chrome/Edge/Firefox/Safari – co najmniej dwie ostatnie wersje),
- stabilne łącze internetowe o przepustowości min. 10 Mb/s (pobieranie) i 2 Mb/s (wysyłanie),
- sprawna kamera komputerowa i mikrofon,
- sprawne słuchawki/ głośniki.

1. **Okres ważności linku:** od godziny zegarowej przed godziną rozpoczęcia szkolenia w dniu pierwszym do godziny zegarowej po zakończeniu szkolenia w dniu ostatnim.

Kontakt

WOJCIECH GRACZYK

E-mail wojciech.graczyk@korycki-graczyk.pl
Telefon (+48) 698 291 420