Możliwość dofinansowania

Cyberbezpieczeństwo dla pracowników biurowych i administracji – szkolenie

Numer usługi 2026/05/31/161638/3599407

4 428,00 PLN brutto
3 600,00 PLN netto
184,50 PLN brutto/h
150,00 PLN netto/h
261,33 PLN cena rynkowa

KORYCKI & GRACZYK CONSULTING GROUP SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

4,9 / 5

835 ocen

Usługa szkoleniowa
zdalna w czasie rzeczywistym
Zajęcia grupowe
24:00 h
10.08.2026 do 12.08.2026

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	2
Maksymalna liczba uczestników	25
Data zakończenia rekrutacji	07-08-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Usługa pn. „Cyberbezpieczeństwo dla pracowników biurowych i administracji – szkolenie” 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
Charakteryzuje podstawowe zasady cyberbezpieczeństwa w pracy biurowej i administracyjnej	Rozróżnia pojęcia na podstawie opisanych sytuacji	Test teoretyczny z wynikiem generowanym automatycznie
	definiuje poufność, integralność i dostępność informacji	Test teoretyczny z wynikiem generowanym automatycznie
	rozróżnia dane, informacje, zasoby i systemy wymagające ochrony	Test teoretyczny z wynikiem generowanym automatycznie
	wskazuje konsekwencje incydentu cyberbezpieczeństwa dla pracownika i organizacji	Test teoretyczny z wynikiem generowanym automatycznie
Identyfikuje podstawowe zasoby cyfrowe i informacyjne wykorzystywane w pracy biurowej	klasyfikuje przykładowe zasoby jako dane osobowe, dokumenty służbowe, dane dostępowe lub zasoby systemowe	Test teoretyczny z wynikiem generowanym automatycznie
	wskazuje, które zasoby wymagają szczególnej ochrony	Test teoretyczny z wynikiem generowanym automatycznie
	dobiera podstawowe środki ochrony do rodzaju zasobu	Test teoretyczny z wynikiem generowanym automatycznie
Rozróżnia najczęstsze zagrożenia cyberbezpieczeństwa dotyczące pracowników biurowych	rozpoznaje phishing, smishing, vishing, fałszywą fakturę, malware, ransomware i próbę wyłudzenia danych	Test teoretyczny z wynikiem generowanym automatycznie
	przyporządkowuje zagrożenie do właściwego przykładu sytuacyjnego	Test teoretyczny z wynikiem generowanym automatycznie
	wskazuje typowe sygnały ostrzegawcze w wiadomości, telefonie lub załączniku	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Dobiera zasady bezpiecznego korzystania z haseł, loginów i uprawnień	rozróżnia hasło silne i słabe na podstawie podanych przykładów	Test teoretyczny z wynikiem generowanym automatycznie
	wskazuje błędy związane z przechowywaniem i powielaniem haseł	Test teoretyczny z wynikiem generowanym automatycznie
	wybiera właściwą metodę tworzenia bezpiecznego hasła	Test teoretyczny z wynikiem generowanym automatycznie
	rozpoznaje ryzyka wynikające z nadmiernych uprawnień użytkownika	Test teoretyczny z wynikiem generowanym automatycznie
Charakteryzuje zasady działania i bezpiecznego używania uwierzytelniania wieloskładnikowego MFA/2FA	wskazuje różnicę między hasłem a dodatkowym składnikiem uwierzytelnienia	Test teoretyczny z wynikiem generowanym automatycznie
	identyfikuje sytuacje, w których nie należy zatwierdzać powiadomienia MFA	Test teoretyczny z wynikiem generowanym automatycznie
	wybiera prawidłową reakcję na niespodziewany kod lub powiadomienie logowania	Test teoretyczny z wynikiem generowanym automatycznie
Wskazuje zasady ochrony urządzenia służbowego i bezpiecznej pracy z oprogramowaniem	rozróżnia działania, które pracownik może wykonać samodzielnie, od działań wymagających kontaktu z IT	Test teoretyczny z wynikiem generowanym automatycznie
	wskazuje rolę aktualizacji systemu i oprogramowania	Test teoretyczny z wynikiem generowanym automatycznie
	identyfikuje przykładowe objawy zainfekowania urządzenia lub przejęcia konta	Test teoretyczny z wynikiem generowanym automatycznie
Dobiera zasady bezpiecznego przesyłania, szyfrowania i przechowywania dokumentów	wybiera prawidłowy sposób przekazania hasła do zaszyfrowanego pliku	Test teoretyczny z wynikiem generowanym automatycznie
	wskazuje zasady minimalizacji danych przy wysyłce dokumentów	Test teoretyczny z wynikiem generowanym automatycznie
	rozpoznaje błędy przy wysyłaniu plików zawierających dane osobowe lub informacje poufne	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje znaczenie kopii zapasowych i zasady bezpiecznego przechowywania danych	definiuje cel wykonywania kopii zapasowej	Test teoretyczny z wynikiem generowanym automatycznie
	wskazuje skutki braku kopii zapasowej w przypadku ransomware	Test teoretyczny z wynikiem generowanym automatycznie
	wybiera prawidłowe zachowanie pracownika dotyczące zapisywania plików na zasobach firmowych	Test teoretyczny z wynikiem generowanym automatycznie
	rozróżnia bezpieczne i ryzykowne miejsca przechowywania danych	Test teoretyczny z wynikiem generowanym automatycznie
Dobiera zasady bezpiecznego korzystania z przeglądarki, sieci Wi-Fi i VPN	wskazuje ograniczenia trybu prywatnego/incognito	Test teoretyczny z wynikiem generowanym automatycznie
	rozpoznaje ryzyka związane z zapamiętywaniem haseł i autologowaniem	Test teoretyczny z wynikiem generowanym automatycznie
	wybiera prawidłowe zachowanie podczas pracy w publicznej sieci Wi-Fi	Test teoretyczny z wynikiem generowanym automatycznie
	wskazuje sytuacje, w których należy użyć VPN	Test teoretyczny z wynikiem generowanym automatycznie
Rozpoznaje incydent bezpieczeństwa i dobiera właściwy sposób jego zgłoszenia	klasyfikuje przykładowe sytuacje jako incydent, podejrzenie incydentu albo zdarzenie niewymagające zgłoszenia	Test teoretyczny z wynikiem generowanym automatycznie
	wskazuje, komu należy zgłosić incydent w organizacji	Test teoretyczny z wynikiem generowanym automatycznie
	wybiera informacje, które powinny znaleźć się w zgłoszeniu incydentu	Test teoretyczny z wynikiem generowanym automatycznie
	rozróżnia działania zalecane i zabronione po wykryciu podejrzanej sytuacji	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Stosuje podstawowe zasady ochrony danych osobowych w pracy biurowej	rozróżnia administratora danych, osobę, której dane dotyczą, przetwarzanie i naruszenie ochrony danych	Test teoretyczny z wynikiem generowanym automatycznie
	wskazuje przykłady naruszeń ochrony danych w pracy biurowej	Test teoretyczny z wynikiem generowanym automatycznie
	dobiera zachowanie zgodne z zasadą minimalizacji danych	Test teoretyczny z wynikiem generowanym automatycznie
	identyfikuje błędy, takie jak wysłanie dokumentu do niewłaściwego odbiorcy, pozostawienie wydruków lub użycie prywatnej skrzynki e-mai	Test teoretyczny z wynikiem generowanym automatycznie
Rozróżnia manipulacje cyfrowe i treści dezinformacyjne tworzone z użyciem AI	wskazuje przykłady deepfake, zmanipulowanego obrazu, fałszywego nagrania lub wygenerowanej wiadomości	Test teoretyczny z wynikiem generowanym automatycznie
	identyfikuje sygnały ostrzegawcze mogące świadczyć o manipulacji treścią	Test teoretyczny z wynikiem generowanym automatycznie
	wybiera prawidłowy sposób weryfikacji podejrzanej informacji przed podjęciem działania służbowego	Test teoretyczny z wynikiem generowanym automatycznie
Charakteryzuje mechanizmy inżynierii społecznej wykorzystywane wobec pracowników biurowych	rozpoznaje techniki wpływu, takie jak presja czasu, autorytet, lęk, poufność, okazja i prośba o pomoc	Test teoretyczny z wynikiem generowanym automatycznie
	przyporządkowuje technikę manipulacji do przykładowej sytuacji	Test teoretyczny z wynikiem generowanym automatycznie
	wybiera prawidłową reakcję na telefon, wiadomość lub prośbę o wykonanie nietypowej czynności służbowej	Test teoretyczny z wynikiem generowanym automatycznie

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

8 godzin zegarowych; 8:00–16:00, w tym łącznie 1 godzina 15 minut przerw: dwie przerwy po 15 minut w pierwszej części dnia, jedna przerwa 30-minutowa oraz jedna przerwa 15-minutowa w drugiej części dnia.

8:00–8:45 – Wprowadzenie do szkolenia — teoria / organizacja

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 — teoria

Definicja „dla ludzi", filary: poufność, integralność, dostępność, dlaczego cyberbezpieczeństwo dotyczy każdego pracownika biurowego, konsekwencje incydentów dla organizacji i pracownika.

09:30–09:45 – Przerwa

09:45–11:15 – Zasoby i zagrożenia — praktyka

Identyfikacja zasobów, takich jak dane osobowe, dokumenty, loginy i dostępy do systemów, najczęstsze zagrożenia, w tym phishing, smishing, vishing, fałszywe faktury i „pilne płatności", praca na case studies.

11:15–11:30 – Przerwa

11:30–13:00 – Pojęcia dla nieinformatyków — teoria

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

13:00–13:30 – Przerwa

13:30–14:15 – „Moje ryzyka w pracy" — praktyka

Indywidualna mapa ryzyk związanych z wykonywanymi zadaniami, w tym pocztą, dokumentami i systemami, praca w parach lub podgrupach, lista najważniejszych ryzyk typowego pracownika biurowego.

14:15–14:30 – Przerwa

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

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

15:15–16:00 – Metody ustalania silnych haseł — praktyka

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

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

8 godzin zegarowych; 8:00–16:00, w tym łącznie 1 godzina 15 minut przerw: dwie przerwy po 15 minut w pierwszej części dnia, jedna przerwa 30-minutowa oraz jedna przerwa 15-minutowa w drugiej części dnia.

8:00–8:45 – Uwierzytelnianie wieloskładnikowe MFA/2FA w praktyce — praktyka

Na czym polega MFA, przebieg logowania krok po kroku, najczęstsze błędy użytkowników, takie jak bezrefleksyjne potwierdzanie logowania i podawanie kodów, krótkie case studies „klikam czy zgłaszam?".

8:45–9:30 – Ochrona urządzenia: programy antywirusowe i aktualizacje — teoria

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

9:30–9:45 – Przerwa

9:45–11:15 – Szyfrowanie dokumentów i plików oraz bezpieczne wysyłanie — praktyka

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

11:15–11:30 – Przerwa

11:30–13:00 – Kopie zapasowe i bezpieczne przechowywanie danych — praktyka

Czym jest backup, jak organizacje go realizują, w tym dyski sieciowe i chmura firmowa w zarysie, rola pracownika, miejsca zapisywania plików, zachowania ryzykowne, minicase „ransomware i brak kopii", checklista zapisywania plików.

13:00–13:30 – Przerwa

13:30–14:15 – Bezpieczne korzystanie z przeglądarki — teoria

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

14:15–14:30 – Przerwa

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

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

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

Typowe objawy problemów z komputerem lub kontem, takie jak dziwne okna, spowolnienie, nietypowe komunikaty, nieoczekiwane wiadomości, co zrobić i czego nie robić, krótkie case studies.

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

8 godzin zegarowych; 8:00–16:00, w tym łącznie 1 godzina 15 minut przerw: dwie przerwy po 15 minut w pierwszej części dnia, jedna przerwa 30-minutowa oraz jedna przerwa 15-minutowa w drugiej części dnia.

8:00–8:45 – Jak zgłaszać incydenty w praktyce — praktyka

Definicja incydentu z perspektywy pracownika, do kogo zgłaszać incydenty, w tym IT, przełożony, IOD, jakie informacje przekazać, przykładowy formularz zgłoszenia incydentu i krótkie ćwiczenie.

8:45–9:30 – RODO z perspektywy pracownika biurowego — teoria

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

9:30–9:45 – Przerwa

9:45–10:30 – Typowe błędy w ochronie danych — praktyka

Analiza kilku naruszeń, takich jak wysłanie wiadomości do złego adresata, pozostawione wydruki, przesyłanie dokumentów na prywatne konto, lista „TOP błędów pracownika biurowego i jak ich unikać".

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

Przykłady deepfake'ów i zniekształconych zdjęć, prosty test rozpoznawania, omówienie, jak generatywna AI ułatwia tworzenie fałszywych treści, w tym maili i dokumentów, oraz jakie znaczenie ma to dla pracownika biurowego.

11:15–11:30 – Przerwa

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

Zasady udostępniania dokumentów osobom trzecim, zasady archiwizacji i niszczenia dokumentów papierowych i elektronicznych, dostęp do systemów z danymi, rozróżnienie działań dozwolonych i niedozwolonych.

12:15–13:00 – Inżynieria społeczna — wprowadzenie — teoria

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

13:00–13:30 – Przerwa

13:30–14:15 – Socjotechnika w praktyce — praktyka

Metody wywierania wpływu na pracowników, typowe scenariusze z biura lub urzędu, takie jak telefon „z banku", „od prezesa" albo „z IT", krótkie scenki i omówienie reakcji.

14:15–14:30 – Przerwa

14:30–15:15 – Phishing w praktyce — praktyka

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

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

Walidacja efektów uczenia się zostanie przeprowadzona w formie testu online w Google Forms. Test obejmuje pytania zamknięte jednokrotnego wyboru odnoszące się do efektów uczenia się i kryteriów ich weryfikacji określonych w Karcie Usługi. Wynik testu generowany jest automatycznie przez system po zakończeniu testu, bez udziału osoby prowadzącej szkolenie w ocenie odpowiedzi. Warunkiem uzyskania pozytywnego wyniku walidacji jest uzyskanie minimum 80% poprawnych odpowiedzi.

Walidacja efektów uczenia się zostanie przeprowadzona w formie testu online w Google Forms. Test obejmuje pytania zamknięte jednokrotnego wyboru odnoszące się do efektów uczenia się i kryteriów ich weryfikacji określonych w Karcie Usługi. Wynik testu generowany jest automatycznie przez system po zakończeniu testu, bez udziału osoby prowadzącej szkolenie w ocenie odpowiedzi. Warunkiem uzyskania pozytywnego wyniku walidacji jest uzyskanie minimum 80% poprawnych odpowiedzi.

1) Godziny i forma

Szkolenie trwa łącznie **24 godziny zegarowe (1 godzina = 60 minut)**. Przerwy wliczane są w czas trwania usługi. Usługa realizowana jest zdalnie w czasie rzeczywistym, na platformie Google Meet. Szkolenie przewidziane jest od dwóch do dwudziestu pięciu osób.

Struktura usługi obejmuje **7 godzin 30 minut części teoretycznej i organizacyjno-teoretycznej**, **12 godzin części praktycznej**, **45 minut walidacji** oraz **3 godziny 45 minut przerw**. Łączny czas trwania usługi wynosi **24 godziny zegarowe**.

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 – szkolenie” 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

Walidacja efektów uczenia się zostanie przeprowadzona po zakończeniu części dydaktycznej szkolenia, w formie testu teoretycznego z wynikiem generowanym automatycznie.

Uczestnik przystępuje do testu samodzielnie, zgodnie z instrukcją przekazaną przed rozpoczęciem walidacji. Test składa się z **co najmniej 30 pytań zamkniętych jednokrotnego wyboru**. Warunkiem uzyskania pozytywnego wyniku walidacji jest uzyskanie minimum 80% poprawnych odpowiedzi.

Harmonogram

Liczba pozycji harmonogramu: 35

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 35 Wprowadzenie do szkolenia – rozmowa na żywo – t	Zajęcia	WOJCIECH GRACZYK	10-08-2026	08:00	08:45	00:45
2 z 35 Podstawy cyberbezpieczeństwa – wideokonferencja – t	Zajęcia	WOJCIECH GRACZYK	10-08-2026	08:45	09:30	00:45
3 z 35 -	Przerwa	-	10-08-2026	09:30	09:45	00:15
4 z 35 Zasoby i zagrożenia – ćwiczenia – p	Zajęcia	WOJCIECH GRACZYK	10-08-2026	09:45	11:15	01:30
5 z 35 -	Przerwa	-	10-08-2026	11:15	11:30	00:15
6 z 35 Pojęcia dla nieinformatyków – wideokonferencja – t	Zajęcia	WOJCIECH GRACZYK	10-08-2026	11:30	13:00	01:30
7 z 35 -	Przerwa	-	10-08-2026	13:00	13:30	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
8 z 35 „Moje ryzyka w pracy” – ćwiczenia – p	Zajęcia	WOJCIECH GRACZYK	10-08-2026	13:30	14:15	00:45
9 z 35 -	Przerwa	-	10-08-2026	14:15	14:30	00:15
10 z 35 Hasła, loginy i uprawnienia – wideokonferencja – t	Zajęcia	WOJCIECH GRACZYK	10-08-2026	14:30	15:15	00:45
11 z 35 Metody ustalania silnych haseł – ćwiczenia – p	Zajęcia	WOJCIECH GRACZYK	10-08-2026	15:15	16:00	00:45
12 z 35 Uwierzytelnianie wieloskładnikowe MFA/2FA w praktyce – ćwiczenia – p	Zajęcia	WOJCIECH GRACZYK	11-08-2026	08:00	08:45	00:45
13 z 35 Ochrona urządzenia: programy antywirusowe i aktualizacje – wideokonferencja – t	Zajęcia	WOJCIECH GRACZYK	11-08-2026	08:45	09:30	00:45
14 z 35 -	Przerwa	-	11-08-2026	09:30	09:45	00:15
15 z 35 Szyfrowanie dokumentów i plików + bezpieczne wysyłanie – ćwiczenia – p	Zajęcia	WOJCIECH GRACZYK	11-08-2026	09:45	11:15	01:30
16 z 35 -	Przerwa	-	11-08-2026	11:15	11:30	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
17 z 35 Kopie zapasowe i bezpieczne przechowywanie danych – ćwiczenia – p	Zajęcia	WOJCIECH GRACZYK	11-08-2026	11:30	13:00	01:30
18 z 35 -	Przerwa	-	11-08-2026	13:00	13:30	00:30
19 z 35 Bezpieczne korzystanie z przeglądarki – wideokonferencja – t	Zajęcia	WOJCIECH GRACZYK	11-08-2026	13:30	14:15	00:45
20 z 35 -	Przerwa	-	11-08-2026	14:15	14:30	00:15
21 z 35 VPN i bezpieczna praca zdalna – ćwiczenia – p	Zajęcia	WOJCIECH GRACZYK	11-08-2026	14:30	15:15	00:45
22 z 35 Objawy incydentu: jak poznać, że „coś jest nie tak” – rozmowa na żywo – p	Zajęcia	WOJCIECH GRACZYK	11-08-2026	15:15	16:00	00:45
23 z 35 Jak zgłaszać incydenty w praktyce – ćwiczenia – p	Zajęcia	WOJCIECH GRACZYK	12-08-2026	08:00	08:45	00:45
24 z 35 RODO z perspektywy pracownika biurowego – wideokonferencja – t	Zajęcia	WOJCIECH GRACZYK	12-08-2026	08:45	09:30	00:45
25 z 35 -	Przerwa	-	12-08-2026	09:30	09:45	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
26 z 35 Typowe błędy w ochronie danych – case studies – p	Zajęcia	WOJCIECH GRACZYK	12-08-2026	09:45	10:30	00:45
27 z 35 Deepfake i inne rozwiązania AI budujące dezinformację – wideokonferencja – t	Zajęcia	WOJCIECH GRACZYK	12-08-2026	10:30	11:15	00:45
28 z 35 -	Przerwa	-	12-08-2026	11:15	11:30	00:15
29 z 35 Praca z dokumentami i systemami w praktyce – ćwiczenia – p	Zajęcia	WOJCIECH GRACZYK	12-08-2026	11:30	12:15	00:45
30 z 35 Inżynieria społeczna — wprowadzenie – wideokonferencja – t	Zajęcia	WOJCIECH GRACZYK	12-08-2026	12:15	13:00	00:45
31 z 35 -	Przerwa	-	12-08-2026	13:00	13:30	00:30
32 z 35 Socjotechnika w praktyce – ćwiczenia – p	Zajęcia	WOJCIECH GRACZYK	12-08-2026	13:30	14:15	00:45
33 z 35 -	Przerwa	-	12-08-2026	14:15	14:30	00:15
34 z 35 Phishing w praktyce – ćwiczenia – p	Zajęcia	WOJCIECH GRACZYK	12-08-2026	14:30	15:15	00:45
35 z 35 -	Walidacja	WOJCIECH GRACZYK	12-08-2026	15:15	16:00	00:45

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	24:00
w tym suma godzin zajęć	19:30
w tym suma godzin walidacji	00:45
w tym suma przerw	03:45
Suma godzin dydaktycznych bez przerw	27:00

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 2024 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	4 428,00 PLN
Koszt przypadający na 1 uczestnika netto	3 600,00 PLN
Koszt osobogodziny brutto	184,50 PLN
Koszt osobogodziny netto	150,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	24:00

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