Możliwość dofinansowania

Cyberbezpieczeństwo i higiena pracy w środowisku zawodowym – usługa szkoleniowa

Numer usługi 2026/04/03/161638/3462833

8 487,00 PLN brutto
6 900,00 PLN netto
212,18 PLN brutto/h
172,50 PLN netto/h
261,33 PLN cena rynkowa

KORYCKI & GRACZYK CONSULTING GROUP SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

4,9 / 5

656 ocen

Usługa szkoleniowa
zdalna w czasie rzeczywistym
40:00 h
11.05.2026 do 14.05.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	• osoby wykonujące zadania administracyjne, organizacyjne i informacyjne • osoby korzystające w codziennej pracy z komputera, poczty elektronicznej, dokumentów i systemów teleinformatycznych • personel biurowy i administracyjny odpowiedzialny za przetwarzanie informacji, dokumentów oraz danych • osoby mające dostęp do danych osobowych, dokumentacji wewnętrznej oraz zasobów organizacji • osoby realizujące obowiązki służbowe w środowisku stacjonarnym, zdalnym lub hybrydowym • osoby, które w swojej pracy korzystają z kont użytkownika, loginów, haseł oraz narzędzi cyfrowych • kadra organizacyjna i administracyjna narażona na ryzyka związane z phishingiem, socjotechniką i błędami w ochronie informacji • osoby, które powinny umieć rozpoznawać zagrożenia cyberbezpieczeństwa oraz prawidłowo reagować na incydenty
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	08-05-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	40

Cel

Cel edukacyjny

Szkolenie "Cyberbezpieczeństwo i higiena pracy w środowisku zawodowym – usługa szkoleniowa" przygotowuje do świadomego i zgodnego z zasadami bezpieczeństwa korzystania z systemów, danych, dokumentów i narzędzi cyfrowych oraz do prawidłowego identyfikowania i zgłaszania incydentów poprzez przekazanie wiedzy merytorycznej oraz wykorzystanie metod praktycznych, w szczególności ćwiczeń i case studies.

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
	Wskazuje kluczowe cechy każdego pojęcia	Test teoretyczny z wynikiem generowanym automatycznie
Rozpoznaje główne grupy zagrożeń typowych dla stanowisk biurowo-administracyjnych	Rozróżnia zagrożenia „ludzkie” od technicznych i organizacyjnych	Test teoretyczny z wynikiem generowanym automatycznie
	Wymienia główne grupy zagrożeń	Test teoretyczny z wynikiem generowanym automatycznie
	Przyporządkowuje przykłady do grup zagrożeń	Test teoretyczny z wynikiem generowanym automatycznie
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	Test teoretyczny z wynikiem generowanym automatycznie
	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

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
	Rozróżnia dobre i złe praktyki na przykładach	Test teoretyczny z wynikiem generowanym automatycznie
Wyróżnia dobre praktyki w obszarze haseł, logowania, pracy zdalnej, nośników danych, korzystania z Wi-Fi i urządzeń mobilnych	Charakteryzuje dobre praktyki w każdym z obszarów	Test teoretyczny z wynikiem generowanym automatycznie
	Uzasadnia spójność dobrych praktyk	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

1)Dzień 1 — Fundamenty cyberbezpieczeństwa i świadomość ryzyk w pracy

10 godzin dydaktycznych | 6:00–14:00

6:00–7:30 – Otwarcie szkolenia i wprowadzenie do cyberbezpieczeństwa

Cel, zakres i zasady pracy podczas szkolenia. Omówienie programu 4-dniowego, zasad pracy stacjonarnej lub on-line, reguł zadawania pytań, kontraktu grupowego oraz poufności przykładów z praktyki uczestników. Wprowadzenie do cyberbezpieczeństwa w ujęciu praktycznym: czym ono jest z perspektywy codziennej pracy i dlaczego dotyczy każdej osoby korzystającej z komputera, poczty i systemów.

7:30–7:45 – Przerwa

7:45–9:15 – Filary bezpieczeństwa informacji i konsekwencje incydentów

Poufność, integralność i dostępność informacji w praktyce. Przekładanie pojęć na codzienne sytuacje: dokumenty, poczta, systemy, rozmowy telefoniczne, praca zdalna. Konsekwencje incydentów dla organizacji, klientów, procesów wewnętrznych oraz osób realizujących zadania administracyjne i organizacyjne.

9:15–10:45 – Zasoby i zagrożenia w codziennej pracy

Identyfikacja zasobów: dane osobowe, dokumenty, loginy, hasła, dostęp do systemów, urządzenia służbowe, korespondencja, wiedza organizacyjna. Omówienie najczęstszych zagrożeń: phishing, smishing, vishing, fałszywe faktury, „pilne płatności", podszywanie się pod przełożonych lub kontrahentów. Praca na przykładach i krótkich case studies.

10:45–11:00 – Przerwa

11:00–12:30 – Pojęcia cyberbezpieczeństwa dla nieinformatyków

Wyjaśnienie podstawowych terminów: malware, ransomware, exploit, podatność, incydent, naruszenie, konto użytkownika, uprawnienia, wyciek danych. Łączenie definicji z realnymi sytuacjami z codziennej praktyki. Miniquiz utrwalający i wspólne porządkowanie pojęć.

12:30–14:00 – „Moje ryzyka w pracy" – warsztat praktyczny

Indywidualna i zespołowa mapa ryzyk związanych z wykonywanymi obowiązkami. Analiza ryzyk w obszarach: poczta elektroniczna, dokumenty, systemy, kontakt z klientem, praca zdalna, przekazywanie danych. Opracowanie listy kluczowych ryzyk dla osób realizujących zadania administracyjne, organizacyjne i informacyjne.

Dzień 2 — Bezpieczny dostęp do systemów i higiena pracy na komputerze

10 godzin dydaktycznych | 6:00–14:00

6:00–7:30 – Hasła, loginy i uprawnienia

Rola loginów, haseł i kont użytkowników w organizacji. Najczęstsze błędy: słabe hasła, powtarzanie tych samych haseł, zapisywanie na kartkach, przekazywanie danych dostępowych innym osobom. Znaczenie uprawnień i zasady korzystania z kont zgodnie z zakresem obowiązków. Omówienie organizacyjnych zasad bezpieczeństwa związanych z dostępem.

7:30–7:45 – Przerwa

7:45–9:15 – Silne hasła w praktyce – ćwiczenia

Zasady tworzenia mocnych, używalnych haseł. Proste metody tworzenia bezpiecznych haseł, np. hasło-zdanie, metoda własnego wzorca, tworzenie unikalnych haseł dla różnych systemów. Omówienie najczęstszych ataków na hasła i ćwiczenia na neutralnych przykładach.

9:15–10:45 – Uwierzytelnianie wieloskładnikowe (MFA/2FA) w praktyce

Na czym polega MFA, jak przebiega logowanie krok po kroku, jakie są najczęstsze błędy użytkowników. Omówienie ryzyka bezrefleksyjnego potwierdzania logowań, podawania kodów osobom trzecim, zatwierdzania prób logowania, których użytkownik nie inicjował. Analiza sytuacji „potwierdzam czy zgłaszam?".

10:45–11:00 – Przerwa

11:00–12:30 – Ochrona urządzenia: antywirus, aktualizacje, podstawowa higiena cyfrowa

Rola narzędzi antywirusowych i antymalware. Znaczenie aktualizacji systemu operacyjnego, przeglądarki i programów użytkowych. Podstawowe sprawdzenie, czy urządzenie działa prawidłowo z perspektywy użytkownika. Co można zrobić samodzielnie, czego nie należy robić bez konsultacji z IT i kiedy niezwłocznie zgłosić problem.

12:30–14:00 – Bezpieczne korzystanie z przeglądarki i codzienne nawyki użytkownika

Tryb prywatny/incognito i jego ograniczenia. Zapamiętywanie haseł w przeglądarce, autologowanie, ciasteczka, rozszerzenia, pobieranie plików i otwieranie linków. Dobre praktyki korzystania z przeglądarki w biurze, w domu oraz podczas pracy na współdzielonym urządzeniu.

Dzień 3 — Bezpieczna praca z danymi, dokumentami i urządzeniami

10 godzin dydaktycznych | 6:00–14:00

6:00–7:30 – Szyfrowanie dokumentów i bezpieczne wysyłanie plików

Szyfrowanie w ujęciu użytkowym: po co jest stosowane i kiedy warto je stosować. Zabezpieczanie dokumentów, archiwów i plików hasłem. Zasady bezpiecznego wysyłania dokumentów: osobny kanał przekazania hasła, weryfikacja adresata, minimalizacja zakresu danych, unikanie pochopnego przekazywania załączników. Wypracowanie prostej procedury bezpiecznej wysyłki.

7:30–7:45 – Przerwa

7:45–9:15 – Kopie zapasowe i bezpieczne przechowywanie danych

Czym jest backup i dlaczego ma znaczenie także z perspektywy codziennej pracy. Podstawowe modele przechowywania danych w organizacji: dyski sieciowe, zasoby współdzielone, chmura firmowa. Rola użytkownika: gdzie zapisywać pliki, czego unikać, jakie praktyki zwiększają bezpieczeństwo i ciągłość pracy. Case study: ransomware, brak kopii i konsekwencje organizacyjne.

9:15–10:45 – VPN i bezpieczna praca zdalna

VPN z perspektywy użytkownika końcowego. Kiedy jest konieczny, jakie ryzyka ogranicza i czego nie rozwiązuje. Praca z domu, podróży, hotelu i publicznego Wi-Fi. Zasady bezpiecznego łączenia się z zasobami organizacji. Ćwiczenie decyzyjne: „łączę się teraz czy czekam i zgłaszam?".

10:45–11:00 – Przerwa

11:00–12:30 – Objawy incydentu: jak rozpoznać, że „coś jest nie tak"

Typowe symptomy problemów na komputerze, koncie lub w skrzynce pocztowej: spowolnienia, podejrzane komunikaty, nietypowe okna, nieautoryzowane logowania, dziwne wiadomości, nietypowe zachowanie systemu lub aplikacji. Co robić, a czego nie robić, aby nie pogorszyć sytuacji. Analiza krótkich scenariuszy incydentowych.

12:30–14:00 – Jak zgłaszać incydenty w praktyce

Definicja incydentu z punktu widzenia użytkownika systemów i narzędzi informatycznych. Ścieżka zgłoszenia: IT, przełożony, IOD, wyznaczone procedury wewnętrzne. Jakie informacje powinny znaleźć się w zgłoszeniu i jak je uporządkować. Ćwiczenie praktyczne na przykładowym formularzu zgłoszeniowym oraz trening krótkiego opisu incydentu.

Dzień 4 — Ochrona danych, socjotechnika, phishing i walidacja

10 godzin dydaktycznych | 6:00–14:00

6:00–7:30 – RODO z perspektywy osoby realizującej zadania administracyjne i organizacyjne

Podstawowe pojęcia: administrator, osoba, której dane dotyczą, przetwarzanie, naruszenie ochrony danych, upoważnienie, minimalizacja danych, zasada „need to know". Omówienie obowiązków w codziennej pracy z dokumentami, wiadomościami i systemami. Przykłady naruszeń w realiach organizacyjnych.

7:30–7:45 – Przerwa

7:45–9:15 – Typowe błędy w ochronie danych i praca z dokumentami w praktyce

Analiza typowych błędów: wysyłka do złego adresata, pozostawione wydruki, przesyłanie dokumentów na prywatne konto, niekontrolowane kopiowanie danych, niewłaściwe udostępnianie plików. Zasady archiwizacji, udostępniania i niszczenia dokumentów papierowych oraz elektronicznych. Opracowanie listy najczęstszych błędów oraz sposobów ich unikania.

9:15–10:45 – Inżynieria społeczna, phishing i manipulacja w środowisku pracy

Czym jest socjotechnika i dlaczego działa. Mechanizmy psychologiczne wykorzystywane przez sprawców: autorytet, presja czasu, lęk, ciekawość, chęć pomocy, rutyna. Typowe scenariusze: telefon „z banku", „od prezesa", „z IT", prośba o pilną płatność, reset hasła, doprecyzowanie danych. Praktyczne rozpoznawanie sygnałów ostrzegawczych.

10:45–11:00 – Przerwa

11:00–12:30 – Deepfake, generatywna AI i nowoczesne formy oszustw

Przykłady fałszywych treści generowanych z użyciem AI: wiadomości e-mail, zdjęcia, dokumenty, głos, wideo. Omówienie, jak AI zwiększa skalę i wiarygodność oszustw oraz jak przekłada się to na bezpieczeństwo codziennej pracy. Prosty trening rozpoznawania sygnałów ostrzegawczych i zasad weryfikacji.

12:30–13:15 – Podsumowanie

13:15 - 14:00 - Walidacja: test teoretyczny z wynikiem generowanym automatycznie

Test wiedzy obejmujący treści szkolenia, realizowany np. w Formularzach Google, z automatycznie generowanym wynikiem. Rekomendowany próg zaliczenia: 80%.

1) Godziny i forma

Szkolenie odbywa się w godzinach dydaktycznych (1 godz. = 45 minut), łącznie **40 godzin dydaktycznych**. Usługa realizowana jest zdalnie, w czasie rzeczywistym, na platformie **Google Meet**. Przerwy (dwie po 15 minut w każdym dniu) nie są wliczane do czasu szkolenia. Grupa: **1–15 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.

- osoby wykonujące zadania administracyjne, organizacyjne i informacyjne
- osoby korzystające w codziennej pracy z komputera, poczty elektronicznej, dokumentów i systemów teleinformatycznych
- personel biurowy i administracyjny odpowiedzialny za przetwarzanie informacji, dokumentów oraz danych
- osoby mające dostęp do danych osobowych, dokumentacji wewnętrznej oraz zasobów organizacji
- osoby realizujące obowiązki służbowe w środowisku stacjonarnym, zdalnym lub hybrydowym
- osoby, które w swojej pracy korzystają z kont użytkownika, loginów, haseł oraz narzędzi cyfrowych
- kadra organizacyjna i administracyjna narażona na ryzyka związane z phishingiem, socjotechniką i błędami w ochronie informacji
- osoby, które powinny umieć rozpoznawać zagrożenia cyberbezpieczeństwa oraz prawidłowo reagować na incydenty

4) Cel edukacyjny. Szkolenie "Cyberbezpieczeństwo i higiena pracy w środowisku zawodowym – usługa szkoleniowa" przygotowuje do świadomego i zgodnego z zasadami bezpieczeństwa korzystania z systemów, danych, dokumentów i narzędzi cyfrowych oraz do prawidłowego identyfikowania i zgłaszania incydentów poprzez przekazanie wiedzy merytorycznej oraz wykorzystanie metod praktycznych, w szczególności ćwiczeń i case studies.

Harmonogram

Liczba pozycji harmonogramu: 29

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 29 Otwarcie szkolenia i wprowadzenie do cyberbezpieczeństwa – wideokonferencja	WOJCIECH GRACZYK	11-05-2026	06:00	07:30	01:30
2 z 29 Przerwa	WOJCIECH GRACZYK	11-05-2026	07:30	07:45	00:15

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
3 z 29 Filary bezpieczeństwa informacji i konsekwencje incydentów – wideokonferencja	WOJCIECH GRACZYK	11-05-2026	07:45	09:15	01:30
4 z 29 Zasoby i zagrożenia w codziennej pracy – współdzielenie ekranu	WOJCIECH GRACZYK	11-05-2026	09:15	10:45	01:30
5 z 29 Przerwa	WOJCIECH GRACZYK	11-05-2026	10:45	11:00	00:15
6 z 29 Pojęcia cyberbezpieczeństwa dla nieinformatyków – wideokonferencja	WOJCIECH GRACZYK	11-05-2026	11:00	12:30	01:30
7 z 29 „Moje ryzyka w pracy” – warsztat praktyczny – ćwiczenia	WOJCIECH GRACZYK	11-05-2026	12:30	14:00	01:30
8 z 29 Hasła, loginy i uprawnienia – wideokonferencja	WOJCIECH GRACZYK	12-05-2026	06:00	07:30	01:30
9 z 29 Przerwa	WOJCIECH GRACZYK	12-05-2026	07:30	07:45	00:15
10 z 29 Silne hasła w praktyce – ćwiczenia	WOJCIECH GRACZYK	12-05-2026	07:45	09:15	01:30
11 z 29 Uwierzytelnianie wieloskładnikowe (MFA/2FA) w praktyce – ćwiczenia	WOJCIECH GRACZYK	12-05-2026	09:15	10:45	01:30
12 z 29 Przerwa	WOJCIECH GRACZYK	12-05-2026	10:45	11:00	00:15

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
13 z 29 Ochrona urządzenia: antywirus, aktualizacje, podstawowa higiena cyfrowa – współdzielenie ekranu	WOJCIECH GRACZYK	12-05-2026	11:00	12:30	01:30
14 z 29 Bezpieczne korzystanie z przeglądarki i codzienne nawyki użytkownika – ćwiczenia	WOJCIECH GRACZYK	12-05-2026	12:30	14:00	01:30
15 z 29 Szyfrowanie dokumentów i bezpieczne wysyłanie plików – ćwiczenia	WOJCIECH GRACZYK	13-05-2026	06:00	07:30	01:30
16 z 29 Przerwa	WOJCIECH GRACZYK	13-05-2026	07:30	07:45	00:15
17 z 29 Kopie zapasowe i bezpieczne przechowywanie danych – współdzielenie ekranu	WOJCIECH GRACZYK	13-05-2026	07:45	09:15	01:30
18 z 29 VPN i bezpieczna praca zdalna – ćwiczenia	WOJCIECH GRACZYK	13-05-2026	09:15	10:45	01:30
19 z 29 Przerwa	WOJCIECH GRACZYK	13-05-2026	10:45	11:00	00:15
20 z 29 Objawy incydentu: jak rozpoznać, że „coś jest nie tak” – współdzielenie ekranu	WOJCIECH GRACZYK	13-05-2026	11:00	12:30	01:30

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
21 z 29 Jak zgłaszać incydenty w praktyce – ćwiczenia	WOJCIECH GRACZYK	13-05-2026	12:30	14:00	01:30
22 z 29 RODO z perspektywy osoby realizującej zadania administracyjne i organizacyjne – wideokonferencja	WOJCIECH GRACZYK	14-05-2026	06:00	07:30	01:30
23 z 29 Przerwa	WOJCIECH GRACZYK	14-05-2026	07:30	07:45	00:15
24 z 29 Typowe błędy w ochronie danych i praca z dokumentami w praktyce – współdzielenie ekranu	WOJCIECH GRACZYK	14-05-2026	07:45	09:15	01:30
25 z 29 Inżynieria społeczna, phishing i manipulacja w środowisku pracy – wideokonferencja	WOJCIECH GRACZYK	14-05-2026	09:15	10:45	01:30
26 z 29 Przerwa	WOJCIECH GRACZYK	14-05-2026	10:45	11:00	00:15
27 z 29 Deepfake, generatywna AI i nowoczesne formy oszustw – ćwiczenia	WOJCIECH GRACZYK	14-05-2026	11:00	12:30	01:30
28 z 29 Podsumowanie – wideokonferencja	WOJCIECH GRACZYK	14-05-2026	12:30	13:15	00:45

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
29 z 29 Walidacja: test teoretyczny z wynikiem generowanym automatycznie	WOJCIECH GRACZYK	14-05-2026	13:15	14:00	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	8 487,00 PLN
Koszt przypadający na 1 uczestnika netto	6 900,00 PLN
Koszt osobogodziny brutto	212,18 PLN
Koszt osobogodziny netto	172,50 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. 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%**.
2. Ocena efektów uczenia się prowadzona jest za pośrednictwem standaryzowanego testu dostępnego online, którego wynik generowany jest automatycznie przez system, **bez udziału człowieka**. Mechanizm walidacji działa niezależnie od procesu szkoleniowego (nie jest obsługiwany przez trenera ani zespół prowadzący), co zapewnia **rozdzielność** obu procesów. Test ma z góry określone progi zaliczeniowe, a wyniki wraz z metadanymi (data/godzina, czas trwania, identyfikator uczestnika) są archiwizowane w systemie, a informacja o rezultacie udostępniana jest uczestnikowi niezwłocznie. Tym samym warunek rozdzielności procesów szkolenia i walidacji pozostaje zachowany. Test składa się z dwudziestu pytań jednokrotnego wyboru (cztery warianty odpowiedzi).

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