Możliwość dofinansowania

Cyberbezpieczeństwo dla pracowników biurowych i administracyjnych — praktyczne szkolenie z cyberhigieny, ochrony danych i reagowania na incydenty

Numer usługi 2026/09/25/161638/3835242

4 920,00 PLN brutto
4 000,00 PLN netto
153,75 PLN brutto/h
125,00 PLN netto/h
261,33 PLN cena rynkowa

KORYCKI & GRACZYK CONSULTING GROUP SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

4,8 / 5

911 ocen

Usługa szkoleniowa
zdalna w czasie rzeczywistym
Zajęcia grupowe
32:00 h
02.11.2026 do 05.11.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikatory projektów	Kierunek - Rozwój, 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. **Szkolenie jest przeznaczone przede wszystkim dla osób chcących chronić dane firmy, rozpoznawać oszustwa np. w mediach społecznościowych oraz odpowiednio reagować na nie.**
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	30
Data zakończenia rekrutacji	01-11-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Podstawa uzyskania wpisu do BUR	Standard Usług Szkoleniowo– Rozwojowych PIFS SUS 3.0

Cel

Cel edukacyjny

Usługa przygotowuje uczestników do świadomego i bezpiecznego funkcjonowania w środowisku cyfrowym poprzez rozwinięcie wiedzy i umiejętności w zakresie rozpoznawania zagrożeń cybernetycznych, ochrony danych i urządzeń, bezpiecznego uwierzytelniania, przeciwdziałania phishingowi i innym oszustwom oraz właściwego reagowania na incydenty bezpieczeństwa.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Omawia podstawowe pojęcia związane z cyberbezpieczeństwem i higieną w sieci, takie jak malware, phishing, bezpieczne hasła i szyfrowanie danych.	Rozróżnia pojęcia na podstawie opisanych sytuacji.	Test teoretyczny z wynikiem generowanym automatycznie
Charakteryzuje różne typy zagrożeń cyfrowych oraz metody ich rozpoznawania.	Rozpoznaje co najmniej trzy typy zagrożeń cyfrowych.	Test teoretyczny z wynikiem generowanym automatycznie
	Przyporządkowuje do typów zagrożeń właściwe przykłady.	Test teoretyczny z wynikiem generowanym automatycznie
	Wskazuje sposoby ich identyfikacji.	Test teoretyczny z wynikiem generowanym automatycznie
Definiuje znaczenie aktualizacji oprogramowania w kontekście zabezpieczeń cyfrowych.	Wyjaśnia znaczenie regularnych aktualizacji dla bezpieczeństwa systemów i danych.	Test teoretyczny z wynikiem generowanym automatycznie
	Rozpoznaje ryzyka wynikające z korzystania z nieaktualnego oprogramowania.	Test teoretyczny z wynikiem generowanym automatycznie
Dobiera zasady tworzenia i zarządzania bezpiecznymi hasłami do opisanych sytuacji zawodowych.	Wskazuje cechy silnego hasła frazowego.	Test teoretyczny z wynikiem generowanym automatycznie
	Rozpoznaje błędy w schematach haseł.	Test teoretyczny z wynikiem generowanym automatycznie
	Wskazuje właściwe zasady korzystania z menedżerów haseł i bezpiecznego przechowywania danych uwierzytelniających.	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozpoznaje próby phishingu i inne oszustwa internetowe oraz dobiera właściwy sposób reagowania.	Rozpoznaje cechy fałszywych wiadomości e-mail, SMS, stron internetowych i innych prób wyłudzenia.	Test teoretyczny z wynikiem generowanym automatycznie
	Wskazuje właściwą kolejność działań w przypadku podejrzenia phishingu, oszustwa lub incydentu bezpieczeństwa.	Test teoretyczny z wynikiem generowanym automatycznie
Rozpoznaje zasady bezpiecznego korzystania z sieci publicznych i prywatnych oraz dobiera odpowiednie sposoby ochrony danych i prywatności.	Identyfikuje ryzyka związane z korzystaniem z sieci publicznych i prywatnych.	Test teoretyczny z wynikiem generowanym automatycznie
	Wskazuje właściwe sposoby ochrony danych, urządzeń i prywatności w opisanych sytuacjach.	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: Wprowadzenie, podstawy prawne, RODO i podstawy zagrożeń

08:00 – 09:00: Wprowadzenie do szkolenia - wideokonferencja — TEORIA (1h)

Kwestie organizacyjne, omówienie celów 4-dniowego programu, kontrakt grupowy oraz zasady zachowania poufności danych organizacji uczestników.

09:00 – 10:00: Samoocena bezpieczeństwa stanowiska pracy - miniaudyt użytkownika - ćwiczenia — PRAKTYKA (1h)

Warsztat z samodzielnej identyfikacji zasobów cyfrowych na stanowisku pracy. Tworzenie uproszczonej mapy ryzyk i podatności stanowiskowych.

10:00 – 10:15: Przerwa (15 min)

10:15 – 11:15: Istota i podstawowe terminy w zakresie cyberbezpieczeństwa - wideokonferencja — TEORIA (1h)

Wyjaśnienie triady poufności, integralności i dostępności (CIA). Omówienie roli pracownika w systemie obrony i skutków finansowo-prawnych wycieków.

11:15 – 12:15: Podstawy prawne cyberbezpieczeństwa i zalecenia ENISA - wideokonferencja — TEORIA (1h)

Przegląd polskich i unijnych regulacji prawnych. Omówienie kluczowych wytycznych Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) dla biur.

12:15 – 12:45: Przerwa (30 min)

12:45 – 13:45: Jak chronić dane osobowe zgodnie z RODO? - wideokonferencja — TEORIA (1h)

Zasady przetwarzania danych w pracy administracyjnej. Identyfikacja ryzyka incydentów i procedury raportowania do Inspektora Ochrony Danych.

13:45 – 14:45: Najpopularniejsze ataki cybernetyczne - ćwiczenia (część 1) — PRAKTYKA (1h)

Analiza studiów przypadku (case studies) dotyczących złośliwego oprogramowania i ransomware.

14:45 – 15:00: Przerwa (15 min)

15:00 – 16:00: Najpopularniejsze ataki cybernetyczne - ćwiczenia (część 2) — PRAKTYKA (1h)

Warsztat z rozpoznawania infekcji komputera oraz dyskusja podsumowująca Dzień 1.

DZIEŃ 2: Phishing, przestępstwa finansowe, socjotechnika, AI i symulacje

08:00 – 09:00: Phishing - ćwiczenia — PRAKTYKA (1h)

Praktyczna detekcja fałszywych wiadomości e-mail i SMS (smishing). Analiza nagłówków, podejrzanych linków oraz technik manipulacji.

09:00 – 10:00: Przestępstwa finansowe w przestrzeni cyfrowej - ćwiczenia — PRAKTYKA (1h)

Rozpracowanie oszustw typu BEC (fałszywe faktury, podmiana kont) oraz mechanizmu wyłudzeń „na prezesa”. Praca na scenariuszach zagrożeń.

10:00 – 10:15: Przerwa (15 min)

10:15 – 11:15: Co o nas wiedzą? - socjotechniki wykorzystywane przez hakerów - wideokonferencja — TEORIA (1h)

Psychologia manipulacji (reguła autorytetu, lęku, pilności). Zagrożenia płynące z białego wywiadu (OSINT) i upubliczniania danych w social mediach.

11:15 – 12:15: Zastrzeż swój PESEL - ćwiczenia — PRAKTYKA (1h)

Instruktaż krok po kroku korzystania z usługi zastrzegania numeru PESEL w aplikacji mObywatel oraz za pośrednictwem właściwej usługi administracji publicznej online. Analiza skutków prawnych ochrony przed wyłudzeniami. Ochrona tożsamości cyfrowej pracownika i przeciwdziałanie wyłudzeniom danych identyfikacyjnych.

12:15 – 12:45: Przerwa (30 min)

12:45 – 13:45: Wykorzystywanie AI przez cyberprzestępców – jak nie dać się nabrać? - wideokonferencja — TEORIA (1h)

Wykorzystanie sztucznej inteligencji do generowania spersonalizowanego phishingu i automatyzacji cyberataków. Nowe wektory zagrożeń.

13:45 – 14:45: Jak rodzą się fake newsy przez wykorzystywanie narzędzi AI? - wideokonferencja — TEORIA (1h)

Mechanizmy dezinformacji. Identyfikacja i zagrożenia związane z materiałami typu Deepfake (fałszowanie głosu przełożonego, wizerunku firmy).

14:45 – 15:00: Przerwa (15 min)

15:00 – 16:00: Ćwiczenie grupowe: symulacje ataków cybernetycznych - ćwiczenia — PRAKTYKA (1h)

Gra symulacyjna (table-top). Podejmowanie decyzji pod presją czasu w sytuacji wielopoziomowego kryzysu naruszenia bezpieczeństwa w biurze.

DZIEŃ 3: Hasła, menedżery haseł, MFA, szyfrowanie i backup

08:00 – 09:00: Zasady ustalania haseł zgodnie z obecnymi standardami bezpieczeństwa cyfrowego - wideokonferencja — TEORIA (1h)

Omówienie nowoczesnych standardów (NIST, KRI). Obalenie mitów o częstej zmianie haseł, zasady konstruowania silnych haseł frazowych.

09:00 – 10:00: Jak działa i jak wybrać menadżera haseł? - wideokonferencja — TEORIA (1h)

Architektura baz haseł, znaczenie hasła głównego (Master Password). Porównanie i kryteria wyboru menadżera haseł do użytku służbowego.

10:00 – 10:15: Przerwa (15 min)

10:15 – 11:15: Dlaczego tak często hakerzy łamią hasła? — TEORIA (1h)

Mechanika ataków słownikowych, brute-force oraz zjawisko wtórnego użycia haseł (credential stuffing).

11:15 – 12:15: Dlaczego tak często hakerzy łamią hasła? — PRAKTYKA (1h)

Analiza zanonimizowanych i syntetycznych przykładów haseł inspirowanych publicznymi raportami o wyciekach, bez wykorzystywania rzeczywistych danych osobowych lub poświadczeń.

12:15 – 12:45: Przerwa (30 min)

12:45 – 13:45: Dlaczego samo hasło nie wystarczy? Uwierzytelnianie dwuskładnikowe (2FA/MFA) w praktyce - wideokonferencja — TEORIA (1h)

Słabości zabezpieczeń jednoskładnikowych. Wprowadzenie do MFA/2FA: omówienie działania aplikacji autoryzujących, kodów i kluczy U2F.

13:45 – 14:45: Szyfrowanie plików, folderów i pendrive'ów w praktyce - ćwiczenia — PRAKTYKA (1h)

Warsztat z obsługi programów szyfrujących (BitLocker, 7-Zip). Procedura bezpiecznej wysyłki załączników i przekazywania haseł innym kanałem.

14:45 – 15:00: Przerwa (15 min)

15:00 – 16:00: Jak robić backup danych? - ćwiczenia — PRAKTYKA (1h)

Wdrożenie reguły 3-2-1 w codziennych obowiązkach. Samodzielne tworzenie kopii zapasowych plików i poczty na dyskach sieciowych według procedury.

DZIEŃ 4: Chmura, ochrona sprzętu/prywatności, obsługa incydentów, kultura, podsumowanie i walidacja

08:00 – 09:00: Dlaczego warto korzystać z „chmury"? - wideokonferencja — TEORIA (1h)

Bezpieczeństwo danych w chmurze (OneDrive, SharePoint) vs serwer lokalny. Zasada współdzielonej odpowiedzialności i kontroli uprawnień.

09:00 – 10:00: Jak zabezpieczyć swój sprzęt i prywatność? Programy antywirusowe, firewall, tryb incognito, cookies, VPN - ćwiczenia — PRAKTYKA (1h)

Konfiguracja podstawowych barier ochronnych na komputerze. Zarządzanie prywatnością w przeglądarce i bezpieczne korzystanie z sieci przez VPN.

10:00 – 10:15: Przerwa (15 min)

10:15 – 12:15: Co zrobić, gdy zostanę zaatakowany? Procedura formalna i komunikacyjna - ćwiczenia — PRAKTYKA (2h)

Trening reagowania na incydent według ścieżki: izolacja sprzętu -> powiadomienie IT -> raport formalny. Praca na schematach blokowych.

12:15 – 12:45: Przerwa (30 min)

12:45 – 13:45: Jak wzmocnić kulturę cyberbezpieczeństwa w organizacji? - wideokonferencja — TEORIA (1h)

Budowanie nawyków zespołowych: blokowanie stacji roboczej (Win+L), zasada czystego biurka/ekranu, bezpieczna utylizacja dokumentów.

13:45 – 14:45: Narzędzia i programy wzmacniające bezpieczeństwo cyfrowe - ćwiczenia — PRAKTYKA (1h)

Dobór i instalacja przydatnych rozszerzeń przeglądarek (blokery skryptów) oraz weryfikacja wycieków poświadczeń w serwisach zewnętrznych.

14:45 – 15:00: Przerwa (15 min)

15:00 – 15:30: Podsumowanie — TEORIA (0,5h)

Sesja Q&A, usystematyzowanie wiedzy z 4 dni szkolenia, ewaluacja i sformułowanie osobistych wniosków wdrożeniowych na stanowisku pracy.

15:30 – 16:00: Test teoretyczny z wynikiem generowanym automatycznie — WALIDACJA (0,5h / 30 min)

Walidacja efektów uczenia się zostanie przeprowadzona w formie testu online w Google Forms, udostępnionego uczestnikom podczas spotkania realizowanego na platformie Google Meet.

1) Godziny i forma

Szkolenie trwa łącznie **32 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 dla grupy od dwóch do trzydziestu osób.

Bilans struktury czasu usługi (4 dni):

- **Część teoretyczna i organizacyjno-teoretyczna:** 13 godzin 30 minut (810 minut)
- **Część praktyczna (warsztaty, ćwiczenia, symulacje):** 14 godzin 00 minut (840 minut)
- **Walidacja (test wiedzy online):** 0 godzin 30 minut (30 minut)
- **Przerwy (ujęte w harmonogramie):** 4 godziny 00 minut (240 minut)
  - **Łączny czas trwania usługi: 32 godziny 00 minut (1920 minut)**

2) Metoda prowadzenia

Zajęcia prowadzone są metodami interaktywnymi i aktywizującymi, umożliwiającymi uczenie się w oparciu o doświadczenie: krótkie wprowadzenia trenera, studia przypadków (*case studies*), ćwiczenia indywidualne i grupowe, quizy online, dyskusje moderowane, odgrywanie scenek sytuacyjnych, praca na checklistach i prostych procedurach biurowych.

3) Grupa docelowa

- 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.

Szkolenie jest przeznaczone przede wszystkim dla osób chcących chronić dane firmy, rozpoznawać oszustwa np. w mediach społecznościowych oraz odpowiednio reagować na nie.

4) Walidacja

Walidacja efektów uczenia się zostanie przeprowadzona w formie testu teoretycznego online z wynikiem generowanym automatycznie. Wynik testu jest ustalany automatycznie na podstawie uprzednio przygotowanego klucza odpowiedzi. Trener nie ocenia odpowiedzi uczestników, nie ingeruje w wynik testu i nie podejmuje decyzji o osiągnięciu efektów uczenia się. Czynności związane z udostępnieniem linku i technicznym uruchomieniem testu nie stanowią oceny efektów uczenia się. Warunkiem zaliczenia walidacji jest uzyskanie co najmniej 80% poprawnych odpowiedzi.

Harmonogram

Liczba pozycji harmonogramu: 40

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 40 Wprowadzenie do szkolenia - wideokonferencja — TEORIA	Zajęcia	DOMINIK HAMERA	02-11-2026	08:00	09:00	01:00
2 z 40 Samoocena bezpieczeństwa stanowiska pracy - miniaudyt użytkownika - ćwiczenia — PRAKTYKA	Zajęcia	DOMINIK HAMERA	02-11-2026	09:00	10:00	01:00
3 z 40 -	Przerwa	-	02-11-2026	10:00	10:15	00:15
4 z 40 Istota i podstawowe terminy w zakresie cyberbezpieczeństwa - wideokonferencja — TEORIA	Zajęcia	DOMINIK HAMERA	02-11-2026	10:15	11:15	01:00
5 z 40 Podstawy prawne cyberbezpieczeństwa i zalecenia ENISA - wideokonferencja — TEORIA	Zajęcia	DOMINIK HAMERA	02-11-2026	11:15	12:15	01:00
6 z 40 -	Przerwa	-	02-11-2026	12:15	12:45	00:30
7 z 40 Jak chronić dane osobowe zgodnie z RODO? - wideokonferencja — TEORIA	Zajęcia	DOMINIK HAMERA	02-11-2026	12:45	13:45	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
8 z 40 Najpopularniejsze ataki cybernetyczne - ćwiczenia (część 1) — PRAKTYKA	Zajęcia	DOMINIK HAMERA	02-11-2026	13:45	14:45	01:00
9 z 40 -	Przerwa	-	02-11-2026	14:45	15:00	00:15
10 z 40 Najpopularniejsze ataki cybernetyczne - ćwiczenia (część 2) — PRAKTYKA	Zajęcia	DOMINIK HAMERA	02-11-2026	15:00	16:00	01:00
11 z 40 Phishing - ćwiczenia — PRAKTYKA	Zajęcia	DOMINIK HAMERA	03-11-2026	08:00	09:00	01:00
12 z 40 Przestępstwa finansowe w przestrzeni cyfrowej - ćwiczenia — PRAKTYKA	Zajęcia	DOMINIK HAMERA	03-11-2026	09:00	10:00	01:00
13 z 40 -	Przerwa	-	03-11-2026	10:00	10:15	00:15
14 z 40 Co o nas wiedzą? - socjotechniki wykorzystywane przez hakerów - wideokonferencja — TEORIA	Zajęcia	DOMINIK HAMERA	03-11-2026	10:15	11:15	01:00
15 z 40 Zastrzeż swój PESEL - ćwiczenia — PRAKTYKA	Zajęcia	DOMINIK HAMERA	03-11-2026	11:15	12:15	01:00
16 z 40 -	Przerwa	-	03-11-2026	12:15	12:45	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
17 z 40 Wykorzystywanie AI przez cyberprzestępców – jak nie dać się nabrać? - wideokonferencja — TEORIA	Zajęcia	DOMINIK HAMERA	03-11-2026	12:45	13:45	01:00
18 z 40 Jak rodzą się fake newsy przez wykorzystywanie narzędzi AI? - wideokonferencja — TEORIA	Zajęcia	DOMINIK HAMERA	03-11-2026	13:45	14:45	01:00
19 z 40 -	Przerwa	-	03-11-2026	14:45	15:00	00:15
20 z 40 Ćwiczenie grupowe: symulacje ataków cybernetycznych - ćwiczenia — PRAKTYKA	Zajęcia	DOMINIK HAMERA	03-11-2026	15:00	16:00	01:00
21 z 40 Zasady ustalania haseł zgodnie z obecnymi standardami bezpieczeństwa cyfrowego - wideokonferencja — TEORIA	Zajęcia	DOMINIK HAMERA	04-11-2026	08:00	09:00	01:00
22 z 40 Jak działa i jak wybrać menadżera haseł? - wideokonferencja — TEORIA	Zajęcia	DOMINIK HAMERA	04-11-2026	09:00	10:00	01:00
23 z 40 -	Przerwa	-	04-11-2026	10:00	10:15	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
24 z 40 Dlaczego tak często hakerzy łamią hasła? — TEORIA	Zajęcia	DOMINIK HAMERA	04-11-2026	10:15	11:15	01:00
25 z 40 Dlaczego tak często hakerzy łamią hasła? — PRAKTYKA	Zajęcia	DOMINIK HAMERA	04-11-2026	11:15	12:15	01:00
26 z 40 -	Przerwa	-	04-11-2026	12:15	12:45	00:30
27 z 40 Dlaczego samo hasło nie wystarczy? Uwierzytelnienie dwuskładnikowe (2FA/MFA) w praktyce - wideokonferencja — TEORIA	Zajęcia	DOMINIK HAMERA	04-11-2026	12:45	13:45	01:00
28 z 40 Szyfrowanie plików, folderów i pendrive'ów w praktyce - ćwiczenia — PRAKTYKA	Zajęcia	DOMINIK HAMERA	04-11-2026	13:45	14:45	01:00
29 z 40 -	Przerwa	-	04-11-2026	14:45	15:00	00:15
30 z 40 Jak robić backup danych? - ćwiczenia — PRAKTYKA	Zajęcia	DOMINIK HAMERA	04-11-2026	15:00	16:00	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
31 z 40 Dlaczego warto korzystać z „chmury”? - wideokonferencja — TEORIA	Zajęcia	DOMINIK HAMERA	05-11-2026	08:00	09:00	01:00
32 z 40 Jak zabezpieczyć swój sprzęt i prywatność? Programy antywirusowe, firewall, tryb incognito... - ćwiczenia — PRAKTYKA	Zajęcia	DOMINIK HAMERA	05-11-2026	09:00	10:00	01:00
33 z 40 -	Przerwa	-	05-11-2026	10:00	10:15	00:15
34 z 40 Co zrobić, gdy zostanę zaatakowany? Procedura formalna i komunikacyjna - ćwiczenia — PRAKTYKA	Zajęcia	DOMINIK HAMERA	05-11-2026	10:15	12:15	02:00
35 z 40 -	Przerwa	-	05-11-2026	12:15	12:45	00:30
36 z 40 Jak wzmocnić kulturę cyberbezpieczeństwa w organizacji? - wideokonferencja — TEORIA	Zajęcia	DOMINIK HAMERA	05-11-2026	12:45	13:45	01:00
37 z 40 Narzędzia i programy wzmacniające bezpieczeństwo cyfrowe - ćwiczenia — PRAKTYKA	Zajęcia	DOMINIK HAMERA	05-11-2026	13:45	14:45	01:00
38 z 40 -	Przerwa	-	05-11-2026	14:45	15:00	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
39 z 40 Podsumowanie — TEORIA	Zajęcia	DOMINIK HAMERA	05-11-2026	15:00	15:30	00:30
40 z 40 -	Walidacja	DOMINIK HAMERA	05-11-2026	15:30	16:00	00:30

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	32:00
w tym suma godzin zajęć	27:30
w tym suma godzin walidacji	00:30
w tym suma przerw	04:00
Suma godzin dydaktycznych bez przerw	37:15

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 2004 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	4 920,00 PLN
Koszt przypadający na 1 uczestnika netto	4 000,00 PLN
Koszt osobogodziny brutto	153,75 PLN
Koszt osobogodziny netto	125,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	32:00

Prowadzący

Liczba prowadzących: 1

1 z 1

DOMINIK HAMERA

Dominik Hamera posiada aktualne i udokumentowane doświadczenie trenerskie z ostatnich 5 lat w obszarze cyberbezpieczeństwa, cyberhigieny, ochrony danych i informacji oraz bezpiecznego korzystania z narzędzi cyfrowych. W 2025 r. przeprowadził łącznie 560 godzin szkoleń z cyberbezpieczeństwa w ramach projektów KPO: 320 h dla mieszkańców woj. śląskiego, 160 h dla mieszkańców woj. wielkopolskiego oraz 80 h dla nauczycieli przedszkoli z woj. kujawsko-pomorskiego. W 2026 r. zrealizował kolejne 240 h szkoleń KPO dla mieszkańców woj. wielkopolskiego. Ponadto przeprowadził ponad 300 h szkoleń dla klientów indywidualnych i firm. Łącznie w latach 2025–2026 zrealizował ponad 1100 h szkoleń związanych z cyberbezpieczeństwem. Zakres obejmował m.in. ochronę danych, phishing, cyberoszustwa, reagowanie na incydenty oraz bezpieczne stosowanie haseł, MFA, backupu, VPN i narzędzi cyfrowych.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały zostaną przekazane drogą elektroniczną. Uczestnik otrzyma skrypty w formacie PDF oraz materiały wideo/linki do materiałów wideo.

Warunki uczestnictwa

Usługa skierowana jest do osób pełnoletnich należących do grupy docelowej wskazanej w Karcie Usługi, w szczególności pracowników administracyjno-biurowych, osób przetwarzających dane oraz osób przygotowujących się do pracy na stanowiskach administracyjnych.

Warunkiem uczestnictwa jest:

- ukończony 18 rok życia,
- podstawowa umiejętność obsługi komputera i poczty elektronicznej,
- dostęp do urządzenia i warunków technicznych umożliwiających udział w szkoleniu online.

Informacje dodatkowe

1. Jeżeli usługa jest finansowana w co najmniej 70% ze środków publicznych, korzysta ze zwolnienia od podatku VAT na podstawie § 3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. (t.j. Dz.U. z 2025 r. poz. 832). W pozostałych przypadkach do ceny netto zostanie doliczony VAT według właściwej stawki.
2. Warunkiem skorzystania z usługi jest udział w co najmniej 80% zajęć merytorycznych, z wyłączeniem czasu przerw, oraz przystąpienie do walidacji efektów uczenia się.

Warunki techniczne

Platforma komunikacyjna

Usługa realizowana jest za pośrednictwem platformy Google Meet. Organizator posiada licencję Google Workspace umożliwiającą prowadzenie spotkań grupowych przez cały czas przewidziany w harmonogramie oraz nagrywanie zajęć.

Test teoretyczny z wynikiem generowanym automatycznie przeprowadzany jest za pośrednictwem Google Forms.

Wymagania sprzętowe

Uczestnik powinien dysponować komputerem stacjonarnym lub laptopem wyposażonym w:

- co najmniej dwurdzeniowy procesor;
- minimum 2 GB pamięci RAM;
- kamerę internetową;
- mikrofon;
- głośniki lub słuchawki.

Dopuszczalny jest udział za pomocą tabletu lub urządzenia mobilnego, jeżeli urządzenie umożliwia korzystanie ze wszystkich funkcji Google Meet i Google Forms niezbędnych do aktywnego uczestnictwa w zajęciach oraz walidacji.

System operacyjny i przeglądarka

Wymagany jest aktualny system operacyjny wspierany przez Google Meet, w szczególności aktualna wersja systemu Microsoft Windows, macOS, Chrome OS albo systemu Linux opartego na dystrybucji Debian.

Uczestnik powinien korzystać z aktualnej wersji jednej z obsługiwanych przeglądarek:

- Google Chrome;
- Microsoft Edge;
- Mozilla Firefox;
- Safari.

Przeglądarka musi mieć włączoną obsługę JavaScript i plików cookies oraz przyznane uprawnienia do korzystania z kamery i mikrofonu.

Połączenie internetowe

Uczestnik powinien posiadać stabilne, szerokopasmowe połączenie z Internetem.

Dla zachowania dobrej jakości obrazu i dźwięku rekomendowane jest łącze o przepustowości co najmniej:

- 4 Mb/s dla pobierania danych;
- 3,2 Mb/s dla wysyłania danych.

W przypadku korzystania z sieci bezprzewodowej zalecane jest przebywanie w miejscu zapewniającym stabilny sygnał Wi-Fi lub skorzystanie z przewodowego połączenia z Internetem.

Adres e-mail i dostęp do usługi

Uczestnik powinien posiadać aktywny adres e-mail umożliwiający otrzymanie:

- linku do spotkań Google Meet;
- materiałów dydaktycznych;
- linku do testu walidacyjnego;
- informacji o wyniku walidacji;
- zabezpieczonego linku do nagrań zajęć.

Link do spotkań Google Meet będzie aktywny od jednej godziny przed rozpoczęciem szkolenia w pierwszym dniu realizacji usługi do jednej godziny po zakończeniu szkolenia w dniu ostatnim.

Link do testu walidacyjnego zostanie udostępniony przed rozpoczęciem walidacji i będzie aktywny w czasie wskazanym w harmonogramie.

Nagrywanie i udostępnianie zajęć

Zajęcia realizowane w głównym pokoju spotkania Google Meet są nagrywane. Nagranie może obejmować prezentowane treści, obraz i głos trenera oraz obraz, głos, nazwę profilu i wypowiedzi uczestników biorących udział w spotkaniu.

Uczestnicy zostaną przed rozpoczęciem usługi poinformowani o zasadach nagrywania, przetwarzania danych i udostępniania nagrań.

Zapoznanie się z nagraniem nie zastępuje udziału w zajęciach prowadzonych w czasie rzeczywistym i nie jest uwzględniane przy obliczaniu frekwencji.

Przygotowanie uczestnika

Przed rozpoczęciem usługi uczestnik powinien sprawdzić:

- możliwość otwarcia linku do Google Meet;
- działanie kamery, mikrofonu i urządzenia odtwarzającego dźwięk;
- stabilność połączenia internetowego;
- możliwość otwarcia formularza Google Forms;
- poprawność adresu e-mail przekazanego organizatorowi.

Kontakt

WOJCIECH GRACZYK

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