Możliwość dofinansowania

Cyberbezpieczeństwo i Higiena w Sieci – usługa szkoleniowa zdalna w czasie rzeczywistym

Numer usługi 2025/05/08/161638/2731936

4 280,40 PLN brutto
3 480,00 PLN netto
147,60 PLN brutto/h
120,00 PLN netto/h

KORYCKI & GRACZYK CONSULTING GROUP SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

★★★★★

zdalna w czasie rzeczywistym
Usługa szkoleniowa
29 h
04.08.2025 do 06.08.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikator projektu	Nowy start w Małopolsce z EURESEM
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	• pracownicy i/lub właściciele pracujący z komputerem, Internetem oraz urządzeniami mobilnymi • pracownicy z sektora MSP • Kadra zarządzająca / menedżerowie • Freelancerzy / twórcy internetowi • uczestnicy projektu Nowy Start w Małopolsce z EURESEM **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	1
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	31-07-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	29

Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Usługa „Cyberbezpieczeństwo i Higiena w Sieci – usługa szkoleniowa zdalna w czasie rzeczywistym” PRZYGOTOWUJE do samodzielnego planowania, wdrażania i utrzymywania praktyk cyberbezpieczeństwa, niezbędnych do ochrony danych i systemów w środowisku zawodowym oraz prywatnym.

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.	Uczestnik poprawnie definiuje wymienione pojęcia i opisuje ich znaczenie w kontekście bezpieczeństwa sieciowego.	Test teoretyczny
	Uczestnik rozróżnia pojęcia w zakresie cyberbezpieczeństwa i ochrony danych osobowych	Test teoretyczny
Stosuje praktyki tworzenia i zarządzania bezpiecznymi hasłami.	Uczestnik demonstruje umiejętność tworzenia silnych haseł i korzystania z menedżerów haseł do ich przechowywania.	Test teoretyczny
	Uczestnik uzasadnia istotę tworzenia silnych haseł	Test teoretyczny
	Uczestnik ocena siłę hasła według kryteriów wskazanych w poleceniu	Test teoretyczny
Uczestnik identyfikuje i reaguje na próby phishingu oraz inne oszustwa internetowe.	Rozpoznaje cechy charakterystyczne fałszywych wiadomości e-mail (np. błędy językowe, fałszywy nadawca, podejrzane linki)	Test teoretyczny
	Identyfikuje niebezpieczne strony internetowe i wyjaśnia, co je odróżnia od bezpiecznych (np. brak certyfikatu HTTPS, nieprawidłowy adres).	Test teoretyczny
	Wskazuje procedury właściwego reagowania na phishing (np. zgłoszenie incydentu, nieklikanie, informowanie działu IT).	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Demonstruje zdolność do krytycznej oceny informacji znalezionych w internecie i ich źródeł	Uczestnik krytycznie ocenia wiarygodność plików multimedialnych (filmów, zdjęć, zrzutów ekranów)	Obserwacja w warunkach symulowanych
Demonstruje zdolność wykonania kopii zapasowej plików	Uczestnik rozróżnia metody tworzenia kopii zapasowej	Test teoretyczny
	Uczestnik charakteryzuje zasady tworzenia skutecznej kopii zapasowej	Test teoretyczny
	Uczestnik organizuje stworzenie kopii zapasowej grupy plików	Obserwacja w warunkach symulowanych
Demonstruje zdolność do wskazania podstaw prawnych ochrony danych osobowych, bezpieczeństwa informacji i cyberbezpieczeństwa	Uczestnik rozróżnia podstawy prawne cyberbezpieczeństwa na poziomie międzynarodowym, unijnym i krajowym	Test teoretyczny
	Uczestnik demonstruje sposób, w jaki wykonuje research podstaw prawnych w zakresie cyberbezpieczeństwa	Obserwacja w warunkach symulowanych
	Uczestnik interpretuje przepisy prawa w zakresie danych osobowych i cyberbezpieczeństwa	Obserwacja w warunkach symulowanych
Demonstruje działanie dwuetapowej autoryzacji	Uczestnik demonstruje, w jaki sposób włącza opcję dwuskładnikowej autoryzacji w mediach społecznościowych grupy Meta	Obserwacja w warunkach symulowanych
	Uczestnik uzasadnia istotę włączenia opcji dwuskładnikowej autoryzacji	Test teoretyczny
Demonstruje działanie programów służących do szyfrowania plików, folderów, dysków	Uczestnik uzasadnia istotę szyfrowania plików	Test teoretyczny
	Uczestnik rozróżnia metody szyfrowania plików, folderów i dysków i wskazuje programy, które do tego służą	Test teoretyczny
	Uczestnik demonstruje, w jaki sposób szyfruje i odblokowuje pliki w formatach PDF, docx, pptx, xlsx.	Obserwacja w warunkach symulowanych
	Uczestnik demonstruje, w jaki sposób wysyła zaszyfrowany plik wraz z podaniem hasła do odbiorcy	Obserwacja w warunkach symulowanych

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

Tak, dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się.

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

Tak, dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji.

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

Tak, dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji.

Program

DZIEŃ PIERWSZY (08:00 - 16:00)

1. **Podstawy cyberbezpieczeństwa**

- Wprowadzenie do Cyberbezpieczeństwa
- Istota i podstawowe terminy w zakresie cyberbezpieczeństwa
- Podstawy prawne cyberbezpieczeństwa i zalecenia ENISA

1. **Cyberataki**

- najpopularniejsze ataki cybernetyczne
- ćwiczenie: phishing
- przestępstwa finansowe w przestrzeni cyfrowej

DZIEŃ DRUGI (08:00 - 16:00)

1. **Hasła i menadżer haseł**

- zasady ustalania haseł zgodnie z obecnymi standardami bezpieczeństwa cyfrowego
- jak działa i jak wybrać menadżera haseł?

1. **Zabezpieczenia przed cyberatakami**

- dlaczego samo hasło nie wystarczy? Autoryzacja dwuskładnikowa w praktyce
- szyfrowanie plików, folderów i pendrive'ów w praktyce
- zastrzeż swój PESEL
- jak robić backup danych?

DZIEŃ TRZECI (08:00 - 16:00)

- podstawowe zasady RODO w zakresie cyberbezpieczeństwa
- jak zabezpieczyć swój sprzęt i prywatność? Programy antywirusowe, firewall, tryb incognito, cookies, VPN
- co o nas wiedzą? - socjotechniki wykorzystywane przez hakerów
- co zrobić, gdy zostanę zaatakowany? Procedura formalna i komunikacyjna
- jak rodzą się fake newsy przez wykorzystywanie narzędzi AI?
- Podsumowanie i najlepsze praktyki

1. **Walidacja**

1) Czas trwania: Szkolenie odbywa się w godzinach dydaktycznych, czyli 1 godzina szkolenia równa się 45 minut, łącznie 29 godzin.

2) Przerwy: Przerwy ujęte w harmonogramie nie są wliczane w czas trwania szkolenia.

3) Metodyka: Prowadzone w ramach szkolenia zajęcia realizowane są metodami interaktywnymi i aktywizującymi, rozumianymi jako metody umożliwiające uczenie się w oparciu o doświadczenie i pozwalające uczestnikom na ćwiczenie umiejętności.

4) Forma: Usługa odbywa się zdalnie w czasie rzeczywistym.

5) Cel edukacyjny: Usługa „Cyberbezpieczeństwo i Higiena w Sieci – usługa szkoleniowa zdalna w czasie rzeczywistym" PRZYGOTOWUJE do samodzielnego planowania, wdrażania i utrzymywania praktyk cyberbezpieczeństwa, niezbędnych do ochrony danych i systemów w środowisku zawodowym oraz prywatnym.

6) Warunki organizacyjne: Szkolenie odbędzie się w formie zdalnej w czasie rzeczywistym na platformie komunikacyjnej Google Meet. Szkolenie przewidziane jest od jednej do piętnastu osób.

7) Walidacja: Proces walidacji składa się z dwóch części: testu teoretycznego oraz obserwacji w warunkach symulowanych. Test teoretyczny polega na wypełnieniu formularza w Google Forms w zakresie tematyki ujętej w efektach uczenia się. Obserwacja w warunkach symulowanych polega na wykonywaniu poleceń związanych z efektami uczenia się, które będą sprawdzane przez walidatora. W przypadku jednego uczestnika walidacja przebiega w terminie wskazanym w harmonogramie, a w przypadku większej liczby uczestników terminy walidacji będą ustalane indywidualnie z uczestnikami. Czas na walidację dla jednej osoby to 60 minut. Dokładne terminy walidacji poszczególnych Uczestników będą dostępne u Dostawcy Usługi.

8) Grupa docelowa:

- pracownicy i/lub właściciele pracujący z komputerem, Internetem oraz urządzeniami mobilnymi
- pracownicy z sektora MSP
- Kadra zarządzająca / menedżerowie
- Freelancerzy / twórcy internetowi
- uczestnicy projektu Nowy Start w Małopolsce z EURESEM
- **Szkolenie jest przeznaczone przede wszystkim dla osób chcących chronić dane firmy, rozpoznawać oszustwa np. w mediach społecznościowych oraz odpowiednio reagować na nie.**

Harmonogram

Liczba przedmiotów/zajęć: 25

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 25 wprowadzenie do szkolenia – wideokonferencja	Wojciech Graczyk	04-08-2025	08:00	09:00	01:00
2 z 25 istota i podstawowe terminy w zakresie cyberbezpieczeństwa – wideokonferencja	Wojciech Graczyk	04-08-2025	09:00	10:00	01:00
3 z 25 przerwa	Wojciech Graczyk	04-08-2025	10:00	10:15	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
4 z 25 podstawy prawne cyberbezpieczeństwa i zalecenia ENISA – współdzielenie ekranu	Wojciech Graczyk	04-08-2025	10:15	11:30	01:15
5 z 25 najpopularniejsze ataki cybernetyczne – wideokonferencja	Wojciech Graczyk	04-08-2025	11:30	13:00	01:30
6 z 25 przerwa	Wojciech Graczyk	04-08-2025	13:00	13:30	00:30
7 z 25 Quiz: phishing – ćwiczenia	Wojciech Graczyk	04-08-2025	13:30	15:00	01:30
8 z 25 przestępstwa finansowe w przestrzeni cyfrowej – współdzielenie ekranu	Wojciech Graczyk	04-08-2025	15:00	16:00	01:00
9 z 25 zasady ustalania haseł zgodnie z obecnymi standardami bezpieczeństwa cyfrowego – chat	Wojciech Graczyk	05-08-2025	08:00	09:00	01:00
10 z 25 jak działa i jak wybrać menadżera haseł? – współdzielenie ekranu	Wojciech Graczyk	05-08-2025	09:00	10:00	01:00
11 z 25 przerwa	Wojciech Graczyk	05-08-2025	10:00	10:15	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
12 z 25 dlaczego samo hasło nie wystarczy? Autoryzacja dwuskładnikowa w praktyce – ćwiczenia	Wojciech Graczyk	05-08-2025	10:15	11:30	01:15
13 z 25 szyfrowanie plików, folderów i pendrive'ów w praktyce – ćwiczenia	Wojciech Graczyk	05-08-2025	11:30	13:00	01:30
14 z 25 przerwa	Wojciech Graczyk	05-08-2025	13:00	13:30	00:30
15 z 25 zastrzeż swój PESEL – ćwiczenia	Wojciech Graczyk	05-08-2025	13:30	15:00	01:30
16 z 25 jak robić backup danych? – ćwiczenia	Wojciech Graczyk	05-08-2025	15:00	16:00	01:00
17 z 25 jak zabezpieczyć swój sprzęt i prywatność? Programy antywirusowe, firewall, tryb incognito, cookies, VPN – współdzielenie ekranu	Wojciech Graczyk	06-08-2025	08:00	09:00	01:00
18 z 25 co o nas wiedzą? - socjotechniki wykorzystywane przez hakerów – chat	Wojciech Graczyk	06-08-2025	09:00	10:00	01:00
19 z 25 przerwa	Wojciech Graczyk	06-08-2025	10:00	10:15	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
20 z 25 co zrobić, gdy zostanę zaatakowany? Procedura formalna i komunikacyjna – współdzielenie ekranu	Wojciech Graczyk	06-08-2025	10:15	11:30	01:15
21 z 25 podstawowe zasady RODO w zakresie cyberbezpieczeństwa – wideokonferencja	Wojciech Graczyk	06-08-2025	11:30	13:00	01:30
22 z 25 przerwa	Wojciech Graczyk	06-08-2025	13:00	13:30	00:30
23 z 25 jak rodzą się fake newsy przez wykorzystywanie narzędzi AI? – współdzielenie ekranu	Wojciech Graczyk	06-08-2025	13:30	14:30	01:00
24 z 25 podsumowanie – chat	Wojciech Graczyk	06-08-2025	14:30	15:00	00:30
25 z 25 Walidacja	-	06-08-2025	15:00	16:00	01:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 280,40 PLN
Koszt przypadający na 1 uczestnika netto	3 480,00 PLN
Koszt osobogodziny brutto	147,60 PLN

Koszt osobogodziny netto	120,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Wojciech Graczyk

Wojciech Graczyk – trener kompetencji miękkich oraz cyfrowych, który podczas swoich szkoleń stawia na praktykę i rezultaty. W ciągu ostatnich pięciu lat przeprowadził ponad 2300 godzin szkoleń, w tym 325 godzin zegarowych w zakresie cyberbezpieczeństwa. Obecnie jest administratorem danych osobowych w spółce pod firmą KORYCKI & GRACZYK CONSULTING GROUP sp. z o.o. oraz jest odpowiedzialny za zabezpieczanie systemów, danych oraz informacji w infrastrukturze firmowej. Ukończył specjalistyczne szkolenia w zakresie zaawansowanych technik cyberbezpieczeństwa ze szczególnym uwzględnieniem prawnych aspektów cyberbezpieczeństwa oraz ustalania haseł. Dodatkowo ukończył kurs w zakresie ochrony danych osobowych na wydziale psychologii i prawa Uniwersytetu SWPS w Poznaniu. Nieustannie podnosi swoje kwalifikacje, uczestnicząc w specjalistycznych szkoleniach, kursach i konferencjach dotyczących prawa zabezpieczenia informacji, RODO, kryptografii oraz higieny w sieci.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Komplet materiałów zostanie wysłany na maila każdego z czestników szkolenia. Będą to podręczniki wraz z prezentacjami danego szkolenia.

Warunki uczestnictwa

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 (próg zdawalności 80%)** oraz **frekwencja na minimalnym poziomie 80%.**
2. Jeśli szkolenie będzie dofinansowane ze środków publicznych w **co najmniej 70%** oraz będzie miało charakter **usługi kształcenia zawodowego lub przekwalifikowania zawodowego,** 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.)).

Warunki techniczne

1. platforma komunikacyjna — Google Meet.

2. wymagania sprzętowe: komputer stacjonarny/laptop, kamera, mikrofon, słuchawki/ głośniki, system operacyjny minimum Windows XP/MacOS High Sierra, min. 2 GB pamięci RAM, pamięć dysku minimum 10 GB,

3. sieć: łącze internetowe minimum 50 kb/s,

4. system operacyjny minimum Windows XP/MacOS High Sierra, przeglądarka internetowa (marka nie ma znaczenia)

5. okres ważności linku: od 1 h przed godziną rozpoczęcia szkolenia w dniu pierwszym do godziny po zakończeniu szkoleń w dniu ostatnim

Kontakt

Wojciech Graczyk

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