Możliwość dofinansowania

Cyberbezpieczeństwo i higiena w sieci – usługa szkoleniowa

Numer usługi 2025/05/26/161638/2771005

6 519,00 PLN brutto
5 300,00 PLN netto
162,98 PLN brutto/h
132,50 PLN netto/h

KORYCKI & GRACZYK CONSULTING GROUP SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

★★★★★

zdalna w czasie rzeczywistym
Usługa szkoleniowa
40 h
30.06.2025 do 03.07.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikator projektu	Małopolski Pociąg do kariery
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	• **Pracownicy firm i instytucji** – zarówno osoby zatrudnione w działach administracji, kadr, marketingu, jak i innych komórkach, które w codziennej pracy korzystają z urządzeń i sieci komputerowych. • **Managerowie i kadra zarządzająca** – odpowiedzialni za bezpieczeństwo danych w firmie, procedury i polityki wewnętrzne. • **Specjaliści i pracownicy działów IT** – osoby techniczne, które chcą usystematyzować wiedzę, pogłębić kompetencje i wdrażać skuteczne zabezpieczenia w organizacjach. • **Osoby odpowiedzialne za zgodność z przepisami (Compliance/Inspektorzy Ochrony Danych/RODO)** – których rolą jest zadbanie o spełnianie wymogów prawnych związanych z ochroną danych osobowych oraz bezpieczeństwem cyfrowym. • **Każda osoba korzystająca z Internetu na co dzień** – która chce chronić swoją tożsamość, finanse oraz prywatność w sieci, niezależnie od poziomu zaawansowania technicznego.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	27-06-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym

Liczba godzin usługi	40
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Usługa „Cyberbezpieczeństwo i Higiena w Sieci” ma na celu zwiększenie świadomości i kompetencji uczestników w zakresie cyberbezpieczeństwa oraz higieny w sieci, z naciskiem na rozumienie i praktyczne stosowanie najlepszych praktyk i strategii obrony przed zagrożeniami cybernetycznymi w środowisku zawodowym i osobistym.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Definiuje podstawowe pojęcia związane z cyberbezpieczeństwem, ochroną danych osobowych i higieną w sieci, takie jak malware, phishing, bezpieczne hasła i szyfrowanie danych.	Uczestnik poprawnie definiuje pojęcia w zakresie bezpieczeństwa cyfrowego, ochrony danych osobowych i higieny w sieci	Test teoretyczny z wynikiem generowanym automatycznie
	Uczestnik rozróżnia pojęcia w zakresie cyberbezpieczeństwa i ochrony danych osobowych	Test teoretyczny z wynikiem generowanym automatycznie
Charakteryzuje różne typy zagrożeń cyfrowych oraz metody ich rozpoznawania.	Uczestnik rozróżnia zagrożenia cyfrowe	Test teoretyczny z wynikiem generowanym automatycznie
	Uczestnik definiuje metody rozpoznawania zagrożeń w sieci	Test teoretyczny z wynikiem generowanym automatycznie
Definiuje znaczenie aktualizacji oprogramowania w kontekście zabezpieczeń cyfrowych.	Uczestnik wyjaśnia, dlaczego regularne aktualizacje oprogramowania są kluczowe dla zachowania bezpieczeństwa systemów i danych.	Test teoretyczny z wynikiem generowanym automatycznie
Stosuje praktyki tworzenia i zarządzania bezpiecznymi hasłami.	Uczestnik definiuje zasady tworzenia silnych haseł	Test teoretyczny z wynikiem generowanym automatycznie
Identyfikuje i reaguje na próby phishingu i inne oszustwa internetowe.	Uczestnik poprawnie identyfikuje fałszywe wiadomości e-mail i strony internetowe oraz zna procedury reagowania na te zagrożenia.	Test teoretyczny z wynikiem generowanym automatycznie
Demonstruje zdolność do krytycznej oceny informacji znalezionych w internecie i ich źródeł	Uczestnik krytycznie ocenia wiarygodność plików multimedialnych (filmów, zdjęć, zrzutów ekranów)	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
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 z wynikiem generowanym automatycznie
	Uczestnik demonstruje sposób, w jaki wykonuje research podstaw prawnych w zakresie cyberbezpieczeństwa	Test teoretyczny z wynikiem generowanym automatycznie
	Uczestnik interpretuje przepisy prawa w zakresie danych osobowych i cyberbezpieczeństwa	Test teoretyczny z wynikiem generowanym automatycznie
	Uczestnik rozróżnia metody tworzenia kopii zapasowej	Test teoretyczny z wynikiem generowanym automatycznie
Demonstruje zdolność wykonania kopii zapasowej plików	Uczestnik charakteryzuje zasady tworzenia skutecznej kopii zapasowej	Test teoretyczny z wynikiem generowanym automatycznie
	Uczestnik organizuje stworzenie kopii zapasowej grupy plików	Test teoretyczny z wynikiem generowanym automatycznie
Demonstruje działanie dwuetapowej autoryzacji	Uczestnik demonstruje, w jaki sposób włącza opcję dwuskładnikowej autoryzacji w mediach społecznościowych grupy Meta	Test teoretyczny z wynikiem generowanym automatycznie
	Uczestnik uzasadnia istotę włączenia opcji dwuskładnikowej autoryzacji	Test teoretyczny z wynikiem generowanym automatycznie
Demonstruje działanie programów służących do szyfrowania plików, folderów, dysków	Uczestnik uzasadnia istotę szyfrowania plików	Test teoretyczny z wynikiem generowanym automatycznie
	Uczestnik rozróżnia metody szyfrowania plików, folderów i dysków i wskazuje programy, które do tego służą	Test teoretyczny z wynikiem generowanym automatycznie

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

DZIEŃ DRUGI (08:00 -16:00)

1. **Przestępstwa finansowe w przestrzeni cyfrowej.**
2. **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

DZIEŃ TRZECI (08:00 - 16:00)

- zastrzeż swój PESEL
- jak robić backup danych?
- jak zabezpieczyć swój sprzęt i prywatność? Programy antywirusowe, firewall, tryb incognito, cookies, VPN
- co o nas wiedzą? - socjotechniki wykorzystywane przez hakerów
- podstawowe zasady RODO w zakresie cyberbezpieczeństwa

DZIEŃ CZWARTY (08:00 - 16:00)

- jak rodzą się fake newsy przez wykorzystywanie narzędzi AI?
- OSINT jako legalny sposób pozyskiwania danych
- co zrobić, gdy zostanę zaatakowany? Procedura formalna i komunikacyjna
- podsumowanie
- **Walidacja**
- Test pisemny

Szkolenie odbywa się w godzinach dydaktycznych, czyli 1 godzina szkolenia równa się 45 minut, łącznie 40 godzin dydaktycznych.

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.

W ciągu dnia są dwie przerwy o łącznej długości 45 minut, które nie wliczają się do czasu trwania usługi.

Harmonogram

Liczba przedmiotów/zajęć: 28

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 28 wprowadzenie do szkolenia	Marta Schneider	30-06-2025	08:00	09:00	01:00
2 z 28 istota i podstawowe terminy w zakresie cyberbezpieczeństwa	Marta Schneider	30-06-2025	09:00	11:00	02:00
3 z 28 przerwa	Marta Schneider	30-06-2025	11:00	11:15	00:15
4 z 28 podstawy prawne cyberbezpieczeństwa i zalecenia ENISA	Marta Schneider	30-06-2025	11:15	13:30	02:15
5 z 28 przerwa	Marta Schneider	30-06-2025	13:30	13:45	00:15
6 z 28 najpopularniejsze ataki cybernetyczne	Marta Schneider	30-06-2025	13:45	15:30	01:45
7 z 28 ćwiczenie: phishing	Marta Schneider	30-06-2025	15:30	16:00	00:30
8 z 28 przestępstwa finansowe w przestrzeni cyfrowej	Marta Schneider	01-07-2025	08:00	10:30	02:30
9 z 28 przerwa	Marta Schneider	01-07-2025	10:30	10:45	00:15
10 z 28 zasady ustalania haseł zgodnie z obecnymi standardami bezpieczeństwa cyfrowego	Marta Schneider	01-07-2025	10:45	13:00	02:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
11 z 28 jak działa i jak wybrać menadżera haseł?	Marta Schneider	01-07-2025	13:00	14:00	01:00
12 z 28 przerwa	Marta Schneider	01-07-2025	14:00	14:15	00:15
13 z 28 dlaczego samo hasło nie wystarczy? Autoryzacja dwuskładnikowa w praktyce	Marta Schneider	01-07-2025	14:15	15:15	01:00
14 z 28 szyfrowanie plików,folderów i pendrive'ów w praktyce	Marta Schneider	01-07-2025	15:15	16:00	00:45
15 z 28 zastrzeż swój PESEL	Marta Schneider	02-07-2025	08:00	08:45	00:45
16 z 28 jak robić backup danych?	Marta Schneider	02-07-2025	08:45	11:00	02:15
17 z 28 przerwa	Marta Schneider	02-07-2025	11:00	11:15	00:15
18 z 28 jak zabezpieczyć swój sprzęt i prywatność? Programy antywirusowe, firewall, tryb incognito, cookies, VPN	Marta Schneider	02-07-2025	11:15	14:00	02:45
19 z 28 przerwa	Marta Schneider	02-07-2025	14:00	14:15	00:15
20 z 28 co o nas wiedzą? - socjotechniki wykorzystywane przez hakerów	Marta Schneider	02-07-2025	14:15	15:00	00:45
21 z 28 podstawowe zasady RODO w zakresie cyberbezpieczeństwa	Marta Schneider	02-07-2025	15:00	16:00	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
22 z 28 jak rodzą się fake newsy przez wykorzystywanie narzędzi AI?	Marta Schneider	03-07-2025	08:00	10:00	02:00
23 z 28 przerwa	Marta Schneider	03-07-2025	10:00	10:15	00:15
24 z 28 OSINT jako legalny sposób pozyskiwania danych	Marta Schneider	03-07-2025	10:15	12:00	01:45
25 z 28 przerwa	Marta Schneider	03-07-2025	12:00	12:15	00:15
26 z 28 co zrobić, gdy zostanę zaatakowany? Procedura formalna i komunikacyjna	Marta Schneider	03-07-2025	12:15	14:30	02:15
27 z 28 podsumowanie	Marta Schneider	03-07-2025	14:30	15:00	00:30
28 z 28 Walidacja – test teoretyczny z wynikami generowanymi automatycznie	Marta Schneider	03-07-2025	15:00	16:00	01:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	6 519,00 PLN
Koszt przypadający na 1 uczestnika netto	5 300,00 PLN
Koszt osobogodziny brutto	162,98 PLN
Koszt osobogodziny netto	132,50 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Marta Schneider

Marta Schneider – trenerka specjalizująca się w kompetencjach cyfrowych i komunikacyjnych. W ciągu ostatnich pięciu lat przeprowadziła ponad 200 godzin zegarowych szkoleń w zakresie cyberbezpieczeństwa i higieny w sieci.
Współpracując z Ośrodkami Pomocy Społecznej, Marta prowadziła wywiady środowiskowe, tworzyła analizy i indywidualne plany pomocy, wspierając klientów w rozwijaniu kompetencji zawodowych. Przepracowała 300 godzin w lokalnych środowiskach, co umożliwiło jej dogłębne poznanie społeczności i podejmowanie szybkich decyzji dla dobrostanu klientów.
Wiedzę specjalistyczną zdobywała na wydziale socjologii Uniwersytetu im. Adama Mickiewicza w Poznaniu na kierunku praca socjalna, na których specjalizowała się w zakresie socjologicznych aspektów dark netu oraz inżynierii społecznej. Na trzecim roku studiów otrzymała stypendium rektora jako osoba, która uzyskała najwyższą średnią na roku.
Uprawnienia trenerskie:
– trener kompetencji miękkich z elementami terapii; skoncentrowanej na rozwiązaniach
– trener-szkoleniowiec w nauczaniu osób dorosłych;
– trener osobisty: coach, mentor tutor z elementami interwencji kryzysowej.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Komplet materiałów zostanie wysłany w wiadomości e-mail dla każdego z uczestników szkolenia.

Zestaw materiałów szkoleniowych składa się z **prezentacji** oraz **skryptu szkolenia**.

Informacje dodatkowe

Uczestnik szkolenia otrzyma zaświadczenie o ukończeniu szkolenia dopiero **po pozytywnym wyniku walidacji**, która składa się z **testu sprawdzającego wiedzę**, który odbędzie się w ostatnim bloku zajęciowym oraz **obserwacji w warunkach symulowanych** kompetencji zdobytych podczas szkolenia. Warunkiem otrzymania zaświadczenia o ukończeniu szkolenia jest pozytywny wynik walidacji (próg zdawalności **80%**) oraz frekwencja na minimalnym poziomie **80%**.

Informujemy również, że szkolenie będzie **nagrywane**!

Jeśli szkolenie będzie dofinansowane ze środków publicznych w **co najmniej70%,** to szkolenie będzie **zwolnione 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