Możliwość dofinansowania

Cyberbezpieczeństwo i Higiena w Sieci – usługa zdalna w czasie rzeczywistym

Numer usługi 2025/04/12/161638/2686708

5 658,00 PLN brutto
4 600,00 PLN netto
217,62 PLN brutto/h
176,92 PLN netto/h

KORYCKI & GRACZYK CONSULTING GROUP SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

★★★★★

zdalna w czasie rzeczywistym
Usługa szkoleniowa
26 h
31.05.2025 do 01.06.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
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 **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	30-05-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	26
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 rozróżnia siłę poszczególnych haseł	Test teoretyczny z wynikiem generowanym automatycznie
	Uczestnik definiuje zasady tworzenia silnych haseł	Test teoretyczny z wynikiem generowanym automatycznie
Identyfikuje i reaguj 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 interpretuje przepisy prawa w zakresie danych osobowych i cyberbezpieczeństwa	Test teoretyczny z wynikiem generowanym automatycznie
Demonstruje zdolność wykonania kopii zapasowej plików	Uczestnik rozróżnia metody tworzenia kopii zapasowej	Test teoretyczny z wynikiem generowanym automatycznie
	Uczestnik charakteryzuje zasady tworzenia skutecznej kopii zapasowej	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 (09:00 - 19:45; 13 godzin dydaktycznych, dwie przerwy po 30 minut)

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

1. **Hasła i menadżer haseł**

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

DZIEŃ DRUGI (09:00 - 19:45; 13 godzin dydaktycznych, dwie przerwy po 30 minut)

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?
- 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**

- Test teoretyczny z wynikami generowanymi automatycznie.

Szkolenie odbywa się w godzinach dydaktycznych, czyli 1 godzina szkolenia równa się 45 minut, łącznie 26 godzin dydaktycznych.

Przerwy nie wliczają się w czas trwania usługi.

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.

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

Minimalne wymagania: Uczestnicy nie muszą posiadać doświadczenia, wiedzy ani umiejętności w zakresie bezpieczeństwa cyfrowego i higieny w sieci.

Harmonogram

Liczba przedmiotów/zajęć: 22

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 22 wprowadzenie do szkolenia – wideokonferencja	Marta Schneider	31-05-2025	09:00	09:45	00:45

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
2 z 22 istota i podstawowe terminy w zakresie cyberbezpieczeństwa – wideokonferencja	Marta Schneider	31-05-2025	09:45	11:00	01:15
3 z 22 podstawy prawne cyberbezpieczeństwa i zalecenia ENISA – wideokonferencja	Marta Schneider	31-05-2025	11:00	12:30	01:30
4 z 22 Przerwa	Marta Schneider	31-05-2025	12:30	13:00	00:30
5 z 22 najpopularniejsze ataki cybernetyczne – wideokonferencja	Marta Schneider	31-05-2025	13:00	14:00	01:00
6 z 22 ćwiczenie: phishing	Marta Schneider	31-05-2025	14:00	15:00	01:00
7 z 22 Przerwa	Marta Schneider	31-05-2025	15:00	15:30	00:30
8 z 22 przestępstwa finansowe w przestrzeni cyfrowej – wideokonferencja	Marta Schneider	31-05-2025	15:30	16:30	01:00
9 z 22 zasady ustalania haseł zgodnie z obecnymi standardami bezpieczeństwa cyfrowego – wideokonferencja	Marta Schneider	31-05-2025	16:30	18:30	02:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
10 z 22 jak działa i jak wybrać menadżera haseł? – współdzielenie ekranu	Marta Schneider	31-05-2025	18:30	19:45	01:15
11 z 22 dlaczego samo hasło nie wystarczy? Autoryzacja dwuskładnikowa w praktyce – warsztaty	Marta Schneider	01-06-2025	09:00	10:00	01:00
12 z 22 szyfrowanie plików, folderów i pendrive'ów w praktyce – warsztaty	Marta Schneider	01-06-2025	10:00	11:00	01:00
13 z 22 Przerwa	Marta Schneider	01-06-2025	11:00	11:30	00:30
14 z 22 zastrzeż swój PESEL – współdzielenie ekranu	Marta Schneider	01-06-2025	11:30	12:00	00:30
15 z 22 jak robić backup danych? – współdzielenie ekranu	Marta Schneider	01-06-2025	12:00	12:30	00:30
16 z 22 jak zabezpieczyć swój sprzęt i prywatność? Programy antywirusowe, firewall, tryb incognito, cookies, VPN – wideokonferencja	Marta Schneider	01-06-2025	12:30	14:00	01:30
17 z 22 co o nas wiedzą? - socjotechniki wykorzystywane przez hakerów – wideokonferencja	Marta Schneider	01-06-2025	14:00	15:00	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
18 z 22 przerwa	Marta Schneider	01-06-2025	15:00	15:30	00:30
19 z 22 co zrobić, gdy zostanę zaatakowany? Procedura formalna i komunikacyjna – współdzielenie ekranu	Marta Schneider	01-06-2025	15:30	17:00	01:30
20 z 22 jak rodzą się fake newsy przez wykorzystywanie narzędzi AI? – współdzielenie ekranu	Marta Schneider	01-06-2025	17:00	18:15	01:15
21 z 22 podsumowanie	Marta Schneider	01-06-2025	18:15	18:45	00:30
22 z 22 Test z wynikiem generowanym automatycznie – walidacja	Marta Schneider	01-06-2025	18:45	19:45	01:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 658,00 PLN
Koszt przypadający na 1 uczestnika netto	4 600,00 PLN
Koszt osobogodziny brutto	217,62 PLN
Koszt osobogodziny netto	176,92 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Marta Schneider

Marta Schneider – trenerka specjalizująca się w kompetencjach cyfrowych i komunikacyjnych. W ciągu ostatnich trzech lat przeprowadziła ponad 550 godzin zegarowych szkoleń z zakresu budowania zespołu i pracy zespołowej, efektywnego poszukiwania pracy w środowisku cyfrowym, marketingu internetowego, bezpieczeństwa cyfrowego oraz efektywnej komunikacji skierowanych do właścicieli i pracowników MMŚP oraz osób dorosłych nieprowadzących działalności gospodarczej, w tym ponad 120 godzin zegarowych z bezpieczeństwa cyfrowego.
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 trzecim roku studiów otrzymała stypendium rektora jako osoba, która uzyskała najwyższą średnią na roku.
Posiada liczne certyfikaty w zakresie marketingu internetowego oraz kompetencji miękkich.
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 na maila każdego z uczestników szkolenia. Będzie to skrypt wraz z prezentacjami danego szkolenia.

Informacje dodatkowe

1. Jeśli szkolenie będzie dofinansowane ze środków publicznych w **co najmniej 70%,** 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.)).
2. Uczestnik szkolenia otrzyma zaświadczenie o ukończeniu szkolenia dopiero po pozytywnym wyniku testu sprawdzającego wiedzę, który odbędzie się na ostatnich zajęciach. Warunkiem otrzymania zaświadczenia o ukończeniu szkolenia jest **pozytywny wynik testu końcowego** oraz **frekwencja na minimalnym poziomie 80%**.
3. Do wybranej metody walidacji nie jest potrzebny walidator, ponieważ uczestnicy dostają link do wypełnienia testu, a wszystkie efekty uczenia się są sprawdzane na podstawie testu z wynikiem generowanym automatycznie. W tej sytuacji zachowuje się rozdzielność między procesem kształcenia a walidacji zgodnie z Regulaminem BUR.

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 1h 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