Możliwość dofinansowania

Szkolenie: Cyberbezpieczeństwo (Małopolski pociąg do kariery – sezon 1)

Numer usługi 2025/04/22/36960/2702212

4 935,15 PLN brutto
4 935,15 PLN netto
88,13 PLN brutto/h
88,13 PLN netto/h

APS Piotr Olgierd Sułkowski

★★★★★

zdalna w czasie rzeczywistym
Usługa szkoleniowa
56 h
10.05.2025 do 18.05.2025

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	Grupą docelową szkolenia są: pracownicy firm i organizacji (wszystkie szczeble), użytkownicy domowi Internetu (bankowość online, media społecznościowe, zakupy), osoby zainteresowane podniesieniem świadomości cyberzagrożeń, kadra zarządzająca, specjaliści IT (perspektywa użytkownika), rodzice/opiekunowie (bezpieczeństwo dzieci online), seniorzy (bezpieczne korzystanie z technologii). Krótko: każdy użytkownik technologii cyfrowych chcący zwiększyć swoje bezpieczeństwo online i ochronę danych. Od uczestników szkolenia nie jest wymagana wiedza ani uprzednie doświadczenie związane ze tematem usługi. Wymagane są natomiast podstawowe umiejętności komunikacyjne. Usługa również adresowana dla Uczestników Projektu MP i/lub dla Uczestników Projektu NSE
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	04-05-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	56

Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Usługa przygotowuje uczestnika do bezpiecznego i świadomego poruszania się w cyfrowym świecie poprzez zrozumienie aktualnych zagrożeń cybernetycznych, poznanie dobrych praktyk ochrony danych i urządzeń (telefon, komputer), bezpiecznego korzystania z mediów społecznościowych i sieci WiFi, tworzenia silnych haseł, rozpoznawania ataków (malware, phishing, ransomware, DDoS), reagowania na incydenty oraz krytycznej oceny informacji (deepfake, dezinformacja).

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Bezpiecznie i świadomie porusza się w cyfrowym świecie	Wyjaśnia rolę sztucznej inteligencji w kontekście cyberbezpieczeństwa (zagrożenia i możliwości).	Obserwacja w warunkach symulowanych
	Zabezpiecza swój telefon zarówno w środowisku domowym, jak i zawodowym, stosując odpowiednie środki ochrony.	Obserwacja w warunkach symulowanych
	Identyfikuje ryzyka związane z korzystaniem z mediów społecznościowych i stosuje dobre praktyki w celu ochrony swoich danych i prywatności.	Obserwacja w warunkach symulowanych
	Definiuje podstawowe pojęcia z zakresu cyberbezpieczeństwa oraz rozpoznaje aktualne zagrożenia w sieci.	Test teoretyczny
	Wymienia i opisuje typowe zagrożenia cybernetyczne w środowisku domowym i zawodowym oraz wdraża odpowiednie środki zaradcze.	Test teoretyczny
	Rozróżnia i opisuje różne rodzaje ataków cybernetycznych, takie jak malware, phishing, ransomware i ataki DDoS.	Test teoretyczny
	Zdefiniuje i wyjaśnia kluczowe pojęcia związane z bezpieczeństwem informacji (poufność, integralność, dostępność, niezaprzeczalność) oraz rozpoznaje definicję incydentu bezpieczeństwa.	Test teoretyczny
	Rozpoznaje symptomy infekcji złośliwym oprogramowaniem na swoich urządzeniach.	Obserwacja w warunkach symulowanych
	Ocenia bezpieczeństwo otwartych sieci WiFi i stosuje bezpieczne praktyki podczas korzystania z nich.	Obserwacja w warunkach symulowanych
	Ochrania swoje dane osobowe i inne informacje podczas korzystania z mediów społecznościowych	Obserwacja w warunkach symulowanych
	Rozróżnia dezinformację od fakenews oraz krytycznie ocenia informacje znalezione w Internecie.	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 -zaświadczenie- 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 potwierdzający uzyskanie kompetencji -zaświadczenie- 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 potwierdzający uzyskanie kompetencji -zaświadczenie- potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji.

Program

1. AI – wróg czy przyjaciel?
2. Ochrona telefonu w domu i pracy
3. Social media -ryzyka i dobre praktyki
4. Podstawy cyberbezpieczeństwa - wprowadzenia w świat cyber - nazwa definicyjna
    1. i znaczenie, aktualne zagrożenia.
5. Cyber w domu – zagrożenia i dobre praktyki
6. Cyber w pracy – zagrożenia i dobre praktyki
7. Rodzaje ataków cybernetycznych: malware, phishing, ransomware, ataki DDoS itp.
8. Podstawowe pojęcia związane z cyberbezpieczeństwem: poufność, integralność, dostępność, poufność, niezaprzeczalność. Definicja incydentu
9. Atrybuty bezpieczeństwa informacji
10. Kim jest haker
11. Elementy bezpieczeństwa cybernetycznego
12. Symptomy infekcji złośliwym oprogramowaniem
13. Co zrobić po infekcji złośliwym oprogramowaniem
14. Czym jest malware i jak się bronić
15. Czym jest ransomware i jak się bronić
16. Czym jest phishing i jak się bronić
17. Czy otwarta sieć WiFi jest bezpieczna
18. Bezpieczeństwo haseł
19. Reguły tworzenia bezpiecznych haseł
20. Ochrona danych w mediach społecznościowych
21. Bezpieczeństwo podczas zakupów internetowych
22. Deepfake
23. Dezinformacja i fakenews
24. Bezpieczeństwo dokumentów
25. Ścieżka zgłaszania incydentu
26. Czy bać się infosfery ?
27. Walidacja

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

Warunki organizacyjne: W celu osiągnięcia maksymalizacji efektów szkolenia, grupa uczestników powinna wynosić minimum 3 osoby.

Szkolenie trwa 56 godzin dydaktycznych . Maksymalna ilość osób w grupie wynosi 20. Realizacja zadań i ćwiczeń będzie przeprowadzona w taki sposób, aby stopniowo narastał ich stopień trudności, ale ich realizacja była w zasięgu możliwości uczestników. Szkolenie przewiduje pracę całej grupy, jak również w podziale na grupy.

Uczestnicy w trakcie każdego dnia szkoleniowego trwającego więcej niż 4 godziny mają prawo do co najmniej 1 przerwy, trwającej co najmniej 15 minut. Przerwy wliczają się w czas trwania usługi.

Po zakończeniu udziału w usłudze rozwojowej, uczestnik otrzymuje odpowiednie zaświadczenie o jej ukończeniu.

Warunkiem uzyskania zaświadczenia jest uczestnictwo w co najmniej 80% zajęć usługi rozwojowej oraz zaliczenie zajęć w formie testu.

1 godzina rozliczeniowa = 45 minut dydaktyczych.

Harmonogram

Liczba przedmiotów/zajęć: 35

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 35 AI – wróg czy przyjaciel? (chat, współdzielenie ekranu, wykład, rozmowa, ćwiczenia)	Ireneusz Pawłowski	10-05-2025	08:00	09:30	01:30
2 z 35 Ochrona telefonu w domu i pracy (chat, współdzielenie ekranu, wykład, rozmowa, ćwiczenia)	Ireneusz Pawłowski	10-05-2025	09:30	11:00	01:30
3 z 35 Social media -ryzyka i dobre praktyki (chat, współdzielenie ekranu, wykład, rozmowa, ćwiczenia)	Ireneusz Pawłowski	10-05-2025	11:00	12:30	01:30
4 z 35 Przerwa	Ireneusz Pawłowski	10-05-2025	12:30	12:45	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 35 Podstawy cyberbezpieczeństwa - wprowadzenia w świat cyber - nazwa definicyjna i znaczenie, aktualne zagrożenia. (chat, współdzielenie ekranu, wykład, rozmowa, ćwiczenia)	Ireneusz Pawłowski	10-05-2025	12:45	14:00	01:15
6 z 35 Cyber w domu – zagrożenia i dobre praktyki (chat, współdzielenie ekranu, wykład, rozmowa, ćwiczenia)	Ireneusz Pawłowski	10-05-2025	14:00	15:30	01:30
7 z 35 Cyber w pracy – zagrożenia i dobre praktyki (chat, współdzielenie ekranu, wykład, rozmowa, ćwiczenia)	Ireneusz Pawłowski	10-05-2025	15:30	16:00	00:30
8 z 35 Cyber w pracy – zagrożenia i dobre praktyki (chat, współdzielenie ekranu, wykład, rozmowa, ćwiczenia)	Ireneusz Pawłowski	11-05-2025	08:00	09:00	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
9 z 35 Rodzaje ataków cybernetycznych: malware, phishing, ransomware, ataki DDoS itp. (chat, współdzielenie ekranu, wykład, rozmowa, ćwiczenia)	Ireneusz Pawłowski	11-05-2025	09:00	10:30	01:30
10 z 35 Podstawowe pojęcia związane z cyberbezpieczeństwem: poufność, integralność, dostępność, poufność, niezaprzeczalność. Definicja incydentu (chat, współdzielenie ekranu, wykład, rozmowa, ćwiczenia)	Ireneusz Pawłowski	11-05-2025	10:30	12:00	01:30
11 z 35 Przerwa	Ireneusz Pawłowski	11-05-2025	12:00	12:15	00:15
12 z 35 Atrybuty bezpieczeństwa informacji (chat, współdzielenie ekranu, wykład, rozmowa, ćwiczenia)	Ireneusz Pawłowski	11-05-2025	12:15	13:30	01:15
13 z 35 Kim jest haker (chat, współdzielenie ekranu, wykład, rozmowa, ćwiczenia)	Ireneusz Pawłowski	11-05-2025	13:30	15:00	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
14 z 35 Elementy bezpieczeństwa cybernetycznego (chat, współdzielenie ekranu, wykład, rozmowa, ćwiczenia)	Ireneusz Pawłowski	11-05-2025	15:00	16:00	01:00
15 z 35 Elementy bezpieczeństwa cybernetycznego (chat, współdzielenie ekranu, wykład, rozmowa, ćwiczenia)	Ireneusz Pawłowski	14-05-2025	17:00	17:30	00:30
16 z 35 Symptomy infekcji złośliwym oprogramowanie m (chat, współdzielenie ekranu, wykład, rozmowa, ćwiczenia)	Ireneusz Pawłowski	14-05-2025	17:30	19:00	01:30
17 z 35 Co zrobić po infekcji złośliwym oprogramowanie m (chat, współdzielenie ekranu, wykład, rozmowa, ćwiczenia)	Ireneusz Pawłowski	14-05-2025	19:00	20:30	01:30
18 z 35 Czym jest malware i jak się bronić (chat, współdzielenie ekranu, wykład, rozmowa, ćwiczenia)	Ireneusz Pawłowski	14-05-2025	20:30	22:00	01:30
19 z 35 Czym jest ransomware i jak się bronić (chat, współdzielenie ekranu, wykład, rozmowa, ćwiczenia)	Ireneusz Pawłowski	15-05-2025	17:00	18:30	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
20 z 35 Czym jest phishing i jak się bronić (chat, współdzielenie ekranu, wykład, rozmowa, ćwiczenia)	Ireneusz Pawłowski	15-05-2025	18:30	20:00	01:30
21 z 35 Czy otwarta sieć WiFi jest bezpieczna (chat, współdzielenie ekranu, wykład, rozmowa, ćwiczenia)	Ireneusz Pawłowski	15-05-2025	20:00	21:30	01:30
22 z 35 Bezpieczeństwo haseł (chat, współdzielenie ekranu, wykład, rozmowa, ćwiczenia)	Ireneusz Pawłowski	15-05-2025	21:30	22:00	00:30
23 z 35 Bezpieczeństwo haseł (chat, współdzielenie ekranu, wykład, rozmowa, ćwiczenia)	Ireneusz Pawłowski	17-05-2025	08:00	09:00	01:00
24 z 35 Reguły tworzenia bezpiecznych haseł (chat, współdzielenie ekranu, wykład, rozmowa, ćwiczenia)	Ireneusz Pawłowski	17-05-2025	09:00	10:30	01:30
25 z 35 Ochrona danych w mediach społecznościowych (chat, współdzielenie ekranu, wykład, rozmowa, ćwiczenia)	Ireneusz Pawłowski	17-05-2025	10:30	12:00	01:30
26 z 35 Przerwa	Ireneusz Pawłowski	17-05-2025	12:00	12:15	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
27 z 35 Bezpieczeństwo podczas zakupów internetowych (chat, współdzielenie ekranu, wykład, rozmowa, ćwiczenia)	Ireneusz Pawłowski	17-05-2025	12:15	13:30	01:15
28 z 35 Deepfake (chat, współdzielenie ekranu, wykład, rozmowa, ćwiczenia)	Ireneusz Pawłowski	17-05-2025	13:30	15:00	01:30
29 z 35 Dezinformacja i fakenews (chat, współdzielenie ekranu, wykład, rozmowa, ćwiczenia)	Ireneusz Pawłowski	17-05-2025	15:00	16:00	01:00
30 z 35 Bezpieczeństwo dokumentów (chat, współdzielenie ekranu, wykład, rozmowa, ćwiczenia)	Ireneusz Pawłowski	18-05-2025	08:00	09:30	01:30
31 z 35 Ścieżka zgłaszania incydentu (chat, współdzielenie ekranu, wykład, rozmowa, ćwiczenia)	Ireneusz Pawłowski	18-05-2025	09:30	12:00	02:30
32 z 35 Przerwa	Ireneusz Pawłowski	18-05-2025	12:00	12:15	00:15
33 z 35 Czy bać się infosfery ? (chat, współdzielenie ekranu, wykład, rozmowa, ćwiczenia)	Ireneusz Pawłowski	18-05-2025	12:15	14:30	02:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
34 z 35 Podsumowanie szkolenia (chat, współdzielenie ekranu, wykład, rozmowa, ćwiczenia)	Ireneusz Pawłowski	18-05-2025	14:30	15:30	01:00
35 z 35 Walidacja	-	18-05-2025	15:30	16:00	00:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 935,15 PLN
Koszt przypadający na 1 uczestnika netto	4 935,15 PLN
Koszt osobogodziny brutto	88,13 PLN
Koszt osobogodziny netto	88,13 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Ireneusz Pawłowski

Ireneusz Pawłowski, Biegły Sądowy z zakresu Bezpieczeństwa Informacji. Audytor systemu ISO 27001:2022. Instruktor Strzelectwa Sportowego. Bardzo sobie ceni 8n lat pracy w największej na świecie firmie security – Brink's. Od kilku lat nadaje ton w Pionie Zarządzania Bezpieczeństwem w Polskim Holdingu Obronnym sp. z o.o. Prywatnie pasjonat militariów i renowacji motocykli.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnikom zostana przekazane materiały dydaktyczne w postacji prezentacji powerpoint, materiały przygotowane przez

trenera, ankiety, testy. Materiały zgodne ze standardem WCAG 2.1.

Warunki uczestnictwa

Wymóg dla uczestników: wyrażenie zgody na przetwarzanie danych osobowych, w tym wizerunku.

Szkolenie w formie zdalnej będzie nagrywane na potrzeby usługodawcy i korzystającego z usługi jak również na potrzeby monitoringu, kontroli oraz w celu utrwalenia efektów kształcenia. Wykorzystanie nagrania na inne cele niż monitoring i kontrola, wymaga pozyskania przez Usługodawcę zgody Uczestnika. Istnieje możliwość udostępnienia nagrań do wglądu Operatora lub innych instytucji nadzorujących.

Informacje dodatkowe

Organizator zapewnia dostępność osobom ze szczególnymi potrzebami podczas realizacji usług rozwojowych zgodnie z Ustawą z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami (Dz.U. 2022 poz. 2240) oraz „Standardami dostępności dla polityki spójności 2021-2027".

W przypadku potrzeby zapewnienia specjalnych udogodnień prosimy o kontakt pod numerem 500 026 554 lub mailem na psulkowski@gmail.com przed zapisem na usługę!

Zawarto umowę z WUP Kraków na rozliczanie usług z wykorzystaniem elektronicznych bonów szkoleniowych w ramach projektu "Małopolski pociąg do kariery - sezon 1" i projektu „Nowy start w Małopolsce z EURESem"

Warunki techniczne

Forma zdalna usługi. Szkolenie prowadzone jest za pośrednictwem platformy ZOOM.US.

1. W celu prawidłowego i pełnego korzystania z usługi, uczestnik powinien dysponować: urządzeniem mającym dostęp do sieci Internet (komputer, smartfon, tablet), zdolnym do odbioru dźwięku (głośniki, słuchawki), zdolnym do przekazywania dźwięku (mikrofon) w celu interakcji pomiędzy trenerem a uczestnikiem, przeglądarką Windows: IE 11+, Edge 12+, Firefox 27+, Chrome 30+, Mac: Safari 7+, Firefox 27+, Chrome 30+.

2. Minimalna wymagana szybkość połączenia internetowego w celu korzystania z webinariów wynosi 2 Mb/s (zalecane połączenie szerokopasmowe).

3. Dołączenie następuje poprzez kliknięcie w indywidualny link wysłany mailem do uczestnika przed analizą oraz wpisanie imienia i nazwiska.

Ważność linku - od rozpoczęcia szkolenia do jego zakończenia zgodnie z harmonogramem w karcie.

Warunki techniczne niezbędne do udziału w usłudze znajdują się pod tym linkiem: https://support.zoom.us/hc/en-us/articles/201362023-System-Requirements-for-PC-Mac-and-Linux

Kontakt

Piotr Sułkowski

E-mail psulkowski@gmail.com
Telefon (+48) 500 026 554