Możliwość dofinansowania

"LIWONA" SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

Brak ocen dla tego dostawcy

Cyberbezpieczeństwo – praktyczny kurs pracy w sieci Internet

Numer usługi 2024/09/27/165415/2332550

5 040,00 PLN brutto
5 040,00 PLN netto
90,00 PLN brutto/h
90,00 PLN netto/h

Wadowice / mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)
Usługa szkoleniowa
56 h
26.11.2024 do 04.12.2024

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikator projektu	Małopolski Pociąg do kariery
Sposób dofinansowania	wsparcie dla osób indywidualnych
Grupa docelowa usługi	Grupą docelową są osoby mieszkające, bądź pracujące w województwie Małopolskim, chcące podnieść swoje kwalifikacje w zakresie cyberbezpieczeństwa. Usługa również adresowana dla uczestników projektu Małopolski pociąg do kariery. Szkolenie kierowane do osób niepełnosprawnych.
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	25
Data zakończenia rekrutacji	25-11-2024
Forma prowadzenia usługi	mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)
Liczba godzin usługi	56
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Usługa "Cyberbezpieczeństwo – praktyczny kurs pracy w sieci Internet" przygotowuje do samodzielnego i bezpiecznego korzystania z sieci Internet, zabezpieczenia swoich danych, weryfikowania informacji, sprawnego posługiwania się najpotrzebniejszymi portalami internetowymi i aplikacjami mobilnymi.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Podopieczny konfiguruje skrzynkę pocztową, ustawia filtry, wysyła załączniki i korzysta z różnych ustawień wiadomości. Rozpoznaje podejrzane e-maile i unika klikania w nieznane linki. Szyfruje wiadomości i korzysta z dwustopniowej weryfikacji. Rozróżnia jakie informacje można bezpiecznie udostępnić przez e-mail.	Uczestnik bezproblemowo posługuje się skrzynką e-mail, dostosowuje ustawienia do swoich preferencji oraz zachowuje swoją prywatność.	Obserwacja w warunkach rzeczywistych
	Podopieczny identyfikuje podejrzane elementy w wiadomościach (np. niezgodność domeny nadawcy, błędy w treści, podejrzane linki).	Obserwacja w warunkach rzeczywistych
	Uczeń definiuje, jak działa proces logowania z dodatkowym zabezpieczeniem.	Obserwacja w warunkach rzeczywistych
Uczeń rozpoznaje wiarygodne źródła informacji, efektywnie wyszukuje potrzebne informacje i rozróżnia, które informacje są zgodne z faktami. Podopieczny rozpoznaje zaufane platformy zakupowe i identyfikuje oznaki niebezpiecznych sklepów. Realizuje płatności w sieci, korzystając z bezpiecznych źródeł płatności.	Uczeń rozróżnia cechy fałszywej lub niewiarygodnej informacji (np. strony bez wskazania autora, brak wiarygodnych odnośników).	Obserwacja w warunkach rzeczywistych
	Podopieczny przechodzi przez proces zakupu w serwisie zakupowym (symulacja), dbając o bezpieczeństwo płatności i ochronę swoich danych osobowych.	Obserwacja w warunkach rzeczywistych
Uczestnik chroni swoje konta, w tym ustawienia prywatności, zabezpieczenia haseł, ograniczenia dostępu do swoich danych i treści dla obcych osób. Rozpoznaje, jakie informacje można bezpiecznie publikować w serwisach społecznościowych, a jakie dane (tj. adresy, zdjęcia rodzinne) powinny być chronione. Rozróżnia podejrzane wiadomości, fałszywe konta, phishing oraz oszustwa w serwisach społecznościowych.	Uczeń przechodzi przez proces ustawiania konta w serwisie społecznościowym, ustawiając odpowiednie opcje prywatności i ograniczenia dostępu do swoich danych.	Obserwacja w warunkach rzeczywistych

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Osoba szkolona zakłada konta i loguje się do aplikacji takich jak ePUAP, PUE-ZUS, mObywatel, Internetowe Konto Pacjenta (IKP), korzystając z bezpiecznych haseł i mechanizmów uwierzytelniania (np. Profil Zaufany). Obsługuje funkcje dostępne w tych aplikacjach, takich jak składanie wniosków online, przeglądanie informacji o stanie konta ZUS, odbieranie e-recept czy sprawdzanie informacji zdrowotnych.	Uczeń loguje się na ePUAP, PUE-ZUS, mObywatel, Internetowe Konto Pacjenta (IKP), wskazuje jak złożyć wniosek, podpisać dokument Profilem Zaufanym, i wysłać go do odpowiedniego urzędu.	Obserwacja w warunkach rzeczywistych
Uczeń rozróżnia, jakie informacje są danymi osobowymi (np. imię, nazwisko, numer PESEL, adres zamieszkania, dane bankowe) i jakie są zagrożenia związane z ich udostępnianiem w Internecie. Stosuje zasady minimalizacji danych, czyli udostępnianie tylko tych informacji, które są absolutnie konieczne. Rozpoznaje próby wyłudzenia danych (phishing, smishing, vishing) oraz odpowiednio zgłasza incydenty związane z próbą wyłudzenia danych.	Uczeń charakteryzuje przykładowe wiadomości phishingowe i pokazuje, jakie elementy wskazują na próbę wyłudzenia danych (np. fałszywe linki, błędy gramatyczne, niezgodności w adresach e-mail).	Obserwacja w warunkach rzeczywistych

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

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?

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?

Dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia walidacji.

Program

Jedna grupa max. 12 osobowa.

Usługa realizowana w godzinach dydaktycznych. Przerwy są wliczone w czas usługi rozwojowej.

-

Dzień 1: E-mail jako podstawowe narzędzie komunikacji w sieci - STANCJONARNE

1.

Podstawy działania poczty email - omówienie

8:00 – 11:00

(w tym przerwa 2 x 15minut)

2.

Warsztaty – założenie darmowego konta e-mail / obsługa skrzynki pocztowej:

- Korzystanie z książki adresowej.
- Redagowanie i wysyłka email.
- Redagowanie stopki / podpisu.
- Odbieranie wiadomości.
- Korzystanie z opcji „odpowiedz do” oraz „odpowiedz wszystkim”.
- Wykorzystywanie korespondencji seryjnej.
- Funkcja adresatów ukrytych.

3.

Bezpieczne hasło

- Omówienie tematyki silnego hasła.
- Omówienie zasady „Ile dostępów tyle haseł”
- Prezentacje i przykłady tworzenia silnych i zarazem prostych haseł.
- Warsztaty – uruchomienie menadżera haseł z wykorzystaniem wcześniej założonych kont.

11:00 – 13:00

(w tym przerwa 2 x 15 minut)

Przerwa obiadowa

13:00 – 13:30

4.

Warsztaty – zabezpieczenie skrzynki e-mail.

- Menadżer haseł – kontynuacja warsztatów
- Omówienie i skonfigurowanie podstawowych zabezpieczeń skrzynki e-mail.
- Uruchomienie opcji uwierzytelnienia dwuskładnikowego.

13:30-16:00

(w tym przerwa 2 x 15 minut)

Dzień 2: Obsługa użytkowych aplikacji mobilnych - STANCJONARNE

1.

Warsztaty EPUAP:

- Logowanie
- Wyszukiwanie urzędów i rodzajów spraw do załatwienia
- Redagowanie i wysłanie pisma do urzędu
- Zarządzanie skrzynką odbiorczą.
- Wersje robocze wiadomości.
- Podpis dokumentu profilem zaufanym

8:00 – 11:00

(w tym przerwa 2 x 15 minut)

2.

Warsztaty PUE-ZUS - wstęp

- Kiedy można skorzystać z PUE.

Warsztaty PUE-ZUS - kontynuacja

- Co można dzięki PUE.
- Inne pokrewne aplikacje - aplikacja mobilna mZUS.

11:00 – 13:00

(w tym przerwa 2 x 15 minut)

3.

Warsztaty mObywatel:

- Instalacja aplikacji i logowanie.
- Pobranie danych dokumentów / aktualizacja dokumentów.
- Przegląd dostępnych usług.
- Usługa „Zastrzeż Pesel”.
- Zgłaszanie incydentów bezpieczeństwa.

Przerwa obiadowa

13:00 – 13:30

4.

Warsztaty IKP (Internetowe Konto Pacjenta)

- Omówienie aplikacji
- Lista dostępnych usług

Inne aplikacje użytkowe.

- Omówienie aplikacji (np. KtoMaLek,GdziePoLek, książki i audiobooki - Storytel, nauka języka – Duolingo)

13:30 – 16:00

(w tym przerwa 2 x 15 minut)

Dzień 3: RODO i praktyczne zasady ochrony swoich danych osobowych - ZDALNIE

1.

Podstawowe informacji na temat ochrony swoich danych osobowych

- Czym są dane osobowe.
- Dlaczego kradną nasze dane osobowe.
- Kiedy musisz podać swoje dane, kiedy urząd / jednostka / placówka publiczna może żądać od ciebie danych.

8:00 - 11:00

(w tym przerwa 2 x 15 minut)

2.

Konsekwencje kradzieży danych osobowych

- Strata finansowa (majątkowa)
- Kradzież tożsamości (podszywanie się pod osobę)
- Strata wizerunkowa

3.

Co zrobić w przypadku kradzieży danych

- Zastrzeżenie pesel
- Zgłoszenie cert, policja
- Zgłoszenie do banku (np. w przypadku kradzieży karty)
- Zmiana haseł (sprawdzenie przekierowania poczty)

11:00 – 13:00

(w tym przerwa 2 x 15 minut)

4.

Techniki manipulacyjne

Omówienie stosowanych metod technik manipulacyjnych i jak się przed nimi bronić

Przerwa obiadowa

13:00 – 13:30

5.

Techniki manipulacyjne – przykłady z omówieniem.

13:30 – 16:00

(w tym przerwa 2 x 15 minut)

Dzień 4: Portale internetowe – ZDALNIE

1.

Rodzaje serwisów internetowych

- Omówienie najpopularniejszych przeglądarek internetowych.
- Nasze działania w sieci a prywatność tego co oglądamy.
- Tryb incognito – do czego się przydaje.

8:00 - 11:00

(w tym przerwa 2x 15 minut)

2.

Serwisy zakupowe

- Obsługa sklepu internetowego.
- Serwisy aukcyjne i ogłoszeniowe.
- Jak bezpiecznie robić zakupy
- Na co zwracać uwagę podczas zakupów i płatności
- Jak oszuści próbują nas podejść podczas zakupów / sprzedaży towarów (omówienie ataków na kupujących / sprzedających)

3.

Serwisy społecznościowe – przegląd najpopularniejszych serwisów społecznościowych

- Omówienie kwestii bezpieczeństwa kont popularnych serwisów społecznościowych.
- Jak wykorzystać strony społecznościowe do zwiększenia swojego bezpieczeństwa.

11:00 – 13:00

(w tym przerwa 2 x 15 minut)

4.

Telefon jako narzędzie do codziennego funkcjonowania w sieci Internet

- Omówienie podstawowych zasad zabezpieczenia telefonu (Android / iPhone).

Przerwa obiadowa

13:00 – 13:30

5.

Telefon jako narzędzie do codziennego funkcjonowania w sieci Internet (kontynuacja)

- Usługa find my phone.
- Kontakty ICE – czym są, jak korzystać.
- Ustawienie informacji medycznej w telefonie (warsztat z ustawienia swoich danych medycznych).

- Mamy Google – udostępnianie lokalizacji
- Aplikacje użytkowe w telefonie – co warto zainstalować.
- Czy płacić telefonem?

13:30 – 16:00

(w tym przerwa 2 x 15 minut)

Dzień 5: RODO i praktyczne zasady ochrony swoich danych osobowych - ZDALNIE

1.

Ochrona wizerunku

- Podstawy prawne.

8:00 - 11:00

(w tym przerwa 2 x 15 minut)

2.

Ochrona wizerunku w sieci – o czym warto pamiętać

- Budowanie swojego wizerunku w sieci.
- Udostępnianie danych w Internecie (w mediach społecznościowych).
- Udostępnianie osób znajomych i bliskich.
- Przegląd profili społecznych, tego co zamieszczamy w Internecie.

3.

Retencja danych – jak usuwać dane i kiedy?

11:00 – 13:00

(w tym przerwa 2 x 15 minut)

4.

Spoofing telefoniczny

- Czym jest spoofing telefoniczny
- Jakie scenariusze mają przestępcy
- Jakie obowiązki mają dostawcy, by utrudnić oszustom spoofing

5.

Telemarketing - jak chronić się na gruncie RODO

- Czym jest telemarketing.
- Przykłady oszustw telemarketingowych
- Jak się uchronić przed oszustwem telemarketerów.

Przerwa obiadowa

13:00 – 13:30

6.

Cyberbezpieczeństwo - Rodzaje zagrożeń w Internecie.

13:30 – 16:00

(w tym przerwa 2 x 15 minut)

Dzień 6: Cyberbezpieczeństwo – STACJONARNE

1.

Phishing, rodzaje i jak się przed nim bronić (przykłady ataków z omówieniem).

8:00-11:00

(w tym przerwa 2 x 15 minut)

2.

Poczta elektroniczna – weryfikacja fałszywych nadawców, linków i załączników.

Warsztat – szyfrowanie załączników

3.

Co zrobić gdy ktoś przejmie skrzynkę mailową – omówienie możliwych scenariuszy i konsekwencji działania atakującego.

4.

Najpopularniejsze (powtarzające się) i aktualne ataki – omówienie przykładów (m.in. Wiadomości sms, atak blik, Atak messenger – przykłady z omówieniem, atak na wnuczka / policjanta / prokuratora / stłuczkę)

11:00 – 13:00

(w tym przerwa 2 x 15 minut)

5.

Komunikatory internetowe (omówienie)

6.

Czy Twoje dane już wyciekły? Omówienie wycieków baz danych loginów i haseł.

Przerwa obiadowa

13:00 – 13:30

7.

Pokaz ataku na żywo:

- Wysłanie maila w czyimś imieniu – jak rozpoznać fałszywą wiadomość.
- Funkcja „odpowiedz do” – na co uważać.

13:30 – 16:00

(w tym przerwa 2 x 15 minut)

8.

Pokaz ataku na żywo:

- wygenerowanie strony internetowej z opcją logowania.
- pokaz łamania haseł

9.

Warsztaty: testy phishingowe – czy jesteś podatny na phishing?

Dzień 7: Cyberbezpieczeństwo – STACJONARNE

1.

Kopia bezpieczeństwa – jak robić, ile kopii robić, gdzie je robić, Czy trzeba robić kopie telefonu?

8:00-11:00

(w tym przerwa 2 x 15 minut)

2.

Nośniki zewnętrzne – na co uważać, jak zabezpieczyć nośnik danych

3.

Aktualizacje oprogramowanie – czy zawsze wgrywać najnowszą wersję systemu? Co i kiedy aktualizować?

4.

Bezpieczna sieć WiFi

- jak chronić własną sieć wifi w domu
- namierzanie i lokalizacja sieci w Internecie

11:00 – 13:00

(w tym przerwa 2 x 15 minut)

5.

Metadane – co można odczytać z dokumentu

6.

Najważniejsze zasady cyberbezpieczeństwa – podsumowanie.

Przerwa obiadowa

13:00 – 13:30

7.

Walidacja szkolenia

13:30 – 16:00

(w tym przerwa 2 x 15 minut)

Harmonogram

Liczba przedmiotów/zajęć: 24

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
1 z 24 Podstawy działania i bezpieczeństwo poczty e-mail - omówienie	Łukasz Polak	26-11-2024	08:00	09:00	01:00	Tak
2 z 24 Warsztaty - założenie darmowego konta e-mail / obsługa skrzynki pocztowej	Łukasz Polak	26-11-2024	09:00	11:00	02:00	Tak

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
3 z 24 Omówienie i prezentacja tematyki silnego hasła, zasady "Ile dostępów tyle haseł", warsztaty - uruchomienie menadżera haseł z wykorzystaniem wcześniej założonych kont	Łukasz Polak	26-11-2024	11:00	13:30	02:30	Tak
4 z 24 Warsztaty zabezpieczenia skrzynki e-mail	Łukasz Polak	26-11-2024	13:30	16:00	02:30	Tak
5 z 24 Warsztaty ePUAP	Urszula Rogalewska	27-11-2024	08:00	10:30	02:30	Tak
6 z 24 Warsztaty PUE-ZUS	Urszula Rogalewska	27-11-2024	10:30	11:30	01:00	Tak
7 z 24 Warsztaty mObywatel	Urszula Rogalewska	27-11-2024	11:30	13:30	02:00	Tak
8 z 24 Warsztaty IKP (Internetowego Konta Pacjenta)	Urszula Rogalewska	27-11-2024	13:30	16:00	02:30	Tak
9 z 24 Podstawowe informacje na temat ochrony swoich danych osobowych, konsekwencje ich kradzieży	Urszula Rogalewska	28-11-2024	08:00	11:00	03:00	Nie

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
10 z 24 Co zrobić w przypadku kradzieży danych. Omówienie stosowanych technik manipulacyjnych	Urszula Rogalewska	28-11-2024	11:00	13:30	02:30	Nie
11 z 24 Techniki manipulacyjne - przykłady z omówieniem	Urszula Rogalewska	28-11-2024	13:30	16:00	02:30	Nie
12 z 24 Rodzaje serwisów internetowych: omówienie, wyszukiwanie informacji, zachowanie prywatności, tryb incognito	Łukasz Polak	29-11-2024	08:00	09:00	01:00	Nie
13 z 24 Serwisy zakupowe: warsztaty praktycznej obsługi sklepów internetowych, omówienie serwisów aukcyjnych i ogłoszeniowych	Łukasz Polak	29-11-2024	09:00	11:00	02:00	Nie

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
14 z 24 Serwisy społecznościowe - przegląd najpopularniejszych serwisów społecznościowych. Telefon jako narzędzie do codziennego funkcjonowania w sieci Internet	Łukasz Polak	29-11-2024	11:00	13:30	02:30	Nie
15 z 24 Telefon jako narzędzie do codziennego funkcjonowania w sieci (kontynuacja)	Łukasz Polak	29-11-2024	13:30	16:00	02:30	Nie
16 z 24 Podstawy prawne ochrony wizerunku. Udostępnianie danych w Internecie. Przegląd zamieszczanych danych.	Urszula Rogalewska	30-11-2024	08:00	11:00	03:00	Nie
17 z 24 Retencja danych - jak i kiedy usuwać dane. Spoofing telefoniczny oraz telemarketing, czyli jak się chronić na gruncie RODO.	Urszula Rogalewska	30-11-2024	11:00	13:30	02:30	Nie

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
18 z 24 Wstęp do cyberbezpieczeństwa. Rodzaje zagrożeń w Internecie.	Urszula Rogalewska	30-11-2024	13:30	16:00	02:30	Nie
19 z 24 Phishing, rodzaje i jak się przed nimi bronić (przykłady ataków z omówieniem). Poczta elektroniczna - weryfikacja fałszywych nadawców, linków i załączników. Przypadki przejęcia skrzynki mailowej.	Łukasz Polak	03-12-2024	08:00	11:00	03:00	Tak
20 z 24 Najpopularniejsze (powtarzające się) i aktualne ataki, przykłady z omówieniem. Komunikatory internetowe. Omówienie wycieków baz danych.	Łukasz Polak	03-12-2024	11:00	13:30	02:30	Tak
21 z 24 Pokaz ataku na żywo. Warsztaty - testy phishingowe	Łukasz Polak	03-12-2024	13:30	16:00	02:30	Tak
22 z 24 Kopia bezpieczeństwa, nośniki zewnętrzne, aktualizacje oprogramowania	Łukasz Polak	04-12-2024	08:00	11:00	03:00	Tak

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
23 z 24 Bezpieczna sieć WiFi. Metadane - co można z nich odczytać. Podsumowanie szkolenia.	Łukasz Polak	04-12-2024	11:00	13:00	02:00	Tak
24 z 24 Walidacja szkolenia	-	04-12-2024	13:00	16:00	03:00	Nie

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 040,00 PLN
Koszt przypadający na 1 uczestnika netto	5 040,00 PLN
Koszt osobogodziny brutto	90,00 PLN
Koszt osobogodziny netto	90,00 PLN

Prowadzący

Liczba prowadzących: 2

1 z 2

Łukasz Polak

W latach 2006-2016 administrator systemów informatycznych w sądownictwie i prokuraturze. Od 10 lat prowadzi własną działalność w zakresie administracji sytemami IT w sektorze prywatnym i publicznym. Ukończył studia informatyczne na Politechnice Łódzkiej a także studia podyplomowe z zakresu cyberbezpieczeństwa. Ukończył również studia podyplomowe w tematyce ochrony danych osobowych w administracji i biznesie. Ponadto wykonuje systemy zabezpieczeń fizycznych takie jak systemy alarmowe, kontroli dostępu czy monitoringu wizyjnego. W związku z realizowanymi projektami został wpisany na listę kwalifikowanych pracowników zabezpieczenia technicznego. Ponadto audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji wg normy PN-EN ISO/IEC 27001 (System Zarządzania Bezpieczeństwem Informacji). W swojej pracy na co dzień administruje infrastrukturami IT klientów ze szczególnym uwzględnieniem bezpieczeństwa danych. Projektuje, wdraża i utrzymuje systemów kopii bezpieczeństwa. Jest czynnym inspektorem ochrony

danych w sektorze publicznym i prywatnym. W swojej pracy niejednokrotnie obsługiwał naruszenia bezpieczeństwa danych zarówno jako obsługa IT jak i inspektor ochrony danych. Posiada autorską dokumentację ochrony informacji, którą z powodzeniem wdraża u swoich klientów. Jednym z elementów systemu bezpieczeństwa jest podnoszenie świadomości pracowników, stąd od wielu lat prowadzi szkolenia z zakresu bezpieczeństwa informacji i cyberbezpieczeństwa.

2 z 2

Urszula Rogalewska

Ukończyła studia na Uniwersytet Śląski w Katowicach, Filia w Cieszynie na kierunku pedagogika, praca socjalna i opiekuńczo – wychowawcza. Uzyskała dyplomy zawodowe i posiada kwalifikacje w zawodzie technik ekonomista oraz technik administracji. Ukończyła studiach podyplomowych Ekonomia społeczna na Uniwersytecie Ekonomicznym w Krakowie oraz studia podyplomowe: „Ochrona danych osobowych" na Akademii Ignatianum w Krakowie. Jest certyfikowanym Audytorem Wiodącym Systemu Zarządzania Bezpieczeństwem Informacji wg normy PN-EN ISO/IEC.
Od 2018 r. czynny Inspektor Ochrony Danych Osobowych w sektorach administracji samorządowej, jak również prywatnych przedsiębiorstwach. Z uwagi na posiadane kompetencje miękkie jak i doświadczenie oraz wiedzę od kilku lat prowadzi szkolenia z zakresu ochrony danych osobowych i bezpieczeństwa informacji zarówno w sektorze publicznym jak i prywatnym.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Po ukończonym szkoleniu zakończonym testem, uczestnicy dostaną zaświadczenie o odbytym szkoleniu oraz certyfikat zdobytych kompetencji.

Informacje dodatkowe

Zaakceptowano Regulamin dla instytucji szkoleniowych.

Warunki techniczne

Minimalne parametry łącza wymaganego do komfortowego uczestnictwa w szkoleniu za pośrednictwem platformy Zoom: 5 Mb/s (przesyłanie) | 3,5 Mb/s (pobieranie)

Minimalne parametry sprzętu:

Procesor : Unisoc SC9832E (4x rdzenie o taktowaniu 1.40 GHz)

Układ graficzny: Mali T820 MP1

Pamięć RAM: 2 GB

Dysk twardy: 32GB

Przekątna i rozdzielczość wyświetlacza: 8.0" 1280x800

Łączność: WiFi i/lub LTE

System operacyjny: Android 13 GO

Adres

ul. Emilii i Karola Wojtyłów 16
34-100 Wadowice
woj. małopolskie

Miejscowość Wadowice, w województwie Małopolskim, ulica Emilii i Karola Wojtyłów, budynek numer 16, po wejściu po schodach na 1 piętro, pierwsze drzwi po lewo, na drzwiach napis "Świetlica"

Udogodnienia w miejscu realizacji usługi

- Wi-fi

Kontakt

Natalia Papuga

E-mail natalia@liwona.pl
Telefon (+48) 500 101 118