Możliwość dofinansowania

Bezpieczeństwo teleinformatyczne rejestratorek i pracowników biurowych w placówkach medycznych - szkolenie.

Numer usługi 2025/12/03/47040/3189286

3 013,50 PLN brutto
2 450,00 PLN netto
188,34 PLN brutto/h
153,13 PLN netto/h

ACTIVEMED SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

5,0 / 5

396 ocen

Gdańsk / stacjonarna
Usługa szkoleniowa
16 h
04.05.2026 do 05.05.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Pracownicy biurowi oraz osoby odpowiedzialne za obszar rejestracji danych w placówce medycznej, niezależnie od ich poziomu doświadczenia z technologią. Szkolenie jest skierowane zarówno do osób, które posiadają podstawową wiedzę z zakresu umiejętności cyfrowych jak i tych, którzy chcą podnieść swoje umiejętności w zakresie bezpieczeństwa teleinformatycznego i kompetencji cyfrowych. Usługa adresowana również do uczestników projektu „Kierunek – Rozwój”.
Minimalna liczba uczestników	6
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	03-05-2026
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	16
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 „Bezpieczeństwo teleinformatyczne rejestratorek i pracowników biurowych w placówkach medycznych - szkolenie” przygotowuje uczestników do samodzielnej i bezpiecznej pracy z systemami IT z zakresu ochrony danych zgodnie z rekomendacjami CEZ i dobrych praktyk.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozróżnia podstawowe rodzaje zagrożeń cybernetycznych występujących w środowisku pracy placówki medycznej.	definiuje pojęcie cyberzagrożenia	Test teoretyczny
	rozróżnia zagrożenia takie jak phishing, malware, botnet, DDoS	Test teoretyczny
	wskazuje przykłady cyberzagrożeń w pracy rejestracji medycznej	Test teoretyczny
Rozpoznaje próby ataków socjotechnicznych w komunikacji elektronicznej.	identyfikuje cechy fałszywych wiadomości e-mail	Test teoretyczny
	wskazuje elementy charakterystyczne dla phishingu	Test teoretyczny
	rozróżnia bezpieczne i niebezpieczne wiadomości	Test teoretyczny
Stosuje zasady bezpiecznego korzystania z Internetu i systemów informatycznych w pracy biurowej.	wskazuje zasady bezpiecznego pobierania plików	Test teoretyczny
	identyfikuje niebezpieczne strony internetowe	Test teoretyczny
	określa zasady bezpiecznego korzystania z poczty elektronicznej	Test teoretyczny
Stosuje zasady ochrony danych wrażliwych w pracy w placówce medycznej.	wskazuje zasady bezpiecznego przetwarzania danych pacjentów	Test teoretyczny
	identyfikuje ryzyka związane z niewłaściwym przetwarzaniem danych	Test teoretyczny
	dobiera właściwe sposoby zabezpieczenia informacji	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Tworzy bezpieczne hasła zgodnie z zasadami bezpieczeństwa informatycznego.	wskazuje elementy silnego hasła	Test teoretyczny
	rozróżnia bezpieczne i niebezpieczne hasła	Test teoretyczny
	dobiera właściwe metody zarządzania hasłami	Test teoretyczny
Stosuje podstawowe zasady zabezpieczenia stanowiska komputerowego.	wskazuje elementy bezpiecznej konfiguracji stanowiska pracy	Test teoretyczny
	identyfikuje zagrożenia wynikające z niewłaściwego zabezpieczenia komputera	Test teoretyczny
	dobiera działania ograniczające ryzyko cyberataku	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

TAK

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

TAK

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

TAK

Program

Program szkolenia

Szkolenie „Bezpieczeństwo teleinformatyczne rejestratorek i pracowników biurowych w placówkach medycznych” skierowane jest do pracowników rejestracji medycznej, pracowników administracyjnych oraz pracowników biurowych podmiotów leczniczych, którzy w swojej pracy korzystają z systemów informatycznych oraz przetwarzają dane pacjentów.

Szkolenie realizowane jest w formie stacjonarnej w grupie od 6 do maksymalnie 15 uczestników. Zajęcia odbywają się w sali szkoleniowej wyposażonej w stanowiska pracy dla wszystkich uczestników, projektor multimedialny, ekran, tablicę typu flipchart oraz dostęp do sieci internetowej. Każdy uczestnik pracuje na własnym laptopie z dostępem do sieci Wi-Fi, co umożliwia wykonywanie ćwiczeń praktycznych.

W trakcie szkolenia uczestnicy wykonują zadania indywidualne oraz ćwiczenia w małych grupach liczących od 2 do 5 osób. Praca zespołowa umożliwia analizę przykładowych sytuacji związanych z cyberzagrożeniami oraz wypracowanie właściwych sposobów reagowania na potencjalne incydenty bezpieczeństwa.

Szkolenie obejmuje łącznie 16 godzin zajęć prowadzonych w trybie godzin zegarowych, przy czym 1 godzina zegarowa odpowiada 1 godzinie dydaktycznej (60 minut).

Struktura szkolenia obejmuje:

- 8 godzin zajęć teoretycznych obejmujących zagadnienia dotyczące cyberzagrożeń, ochrony danych oraz zasad bezpieczeństwa pracy z systemami informatycznymi,
- 8 godzin zajęć praktycznych obejmujących analizę przypadków, ćwiczenia indywidualne oraz ćwiczenia realizowane w grupach.

W trakcie szkolenia przewidziane są przerwy organizacyjne (przerwy kawowe oraz przerwa obiadowa), które są wliczane do czasu trwania zajęć dydaktycznych.

Walidacja efektów uczenia się przeprowadzana jest po zakończeniu szkolenia w formie testu wiedzy obejmującego zagadnienia omawiane podczas szkolenia. Test pozwala zweryfikować stopień osiągnięcia efektów uczenia się określonych w karcie usługi. Proces walidacji prowadzony jest przez osobę wyznaczoną do przeprowadzenia walidacji, inną niż trener prowadzący szkolenie, co zapewnia rozdzielenie procesu kształcenia od procesu walidacji.

Dzień 1: Cyberzagrożenia i podstawy bezpieczeństwa teleinformatycznego w pracy rejestratorek i pracowników biurowych placówek medycznych.

1. Powitanie i rejestracja uczestników.
2. Wprowadzenie do cyberbezpieczeństwa w kontekście środowiska medycznego i biurowego w placówkach medycznych.
3. Analiza aktualnych zagrożeń w sieciach informatycznych w kontekście pracy rejestratorek i pracowników biurowych w placówkach medycznych.
4. Przerwa kawowa.
5. Podstawowe zasady bezpieczeństwa danych medycznych.
6. Cyberatak i jego skutki dla placówek medycznych.
7. Rola rejestratorki i sekretarki medycznej w utrzymaniu bezpieczeństwa informacji.
8. Przerwa obiadowa.
9. Metody ochrony przed atakami phishingowymi i socjotechnicznymi w aspekcie pracy placówek medycznych.
10. Szkolenie praktyczne: rozpoznawanie prób phishingu.
11. Przerwa kawowa.
12. Wprowadzenie do zabezpieczeń haseł i kont w kontekście pracy i bezpieczeństwa placówek medycznych.
13. Rola silnych haseł w ochronie danych.
14. Ćwiczenia praktyczne: tworzenie bezpiecznych haseł.

Dzień 2: Zarządzanie ryzykiem i narzędzia bezpieczeństwa w funkcjonowaniu placówek medycznych.

1. Analiza ryzyka w kontekście środowiska medycznego.
2. Planowanie strategii bezpieczeństwa informatycznego dla placówek medycznych.
3. Szkolenie praktyczne: tworzenie polityki bezpieczeństwa, procedury postępowania.
4. Przerwa kawowa.
5. Rola rejestratorki i sekretarki medycznej w zabezpieczaniu informacji pacjentów.
6. Znaczenie zabezpieczeń sprzętowych i programowych w bezpiecznym funkcjonowaniu placówki medycznej.
7. Szkolenie praktyczne: instalacja i konfiguracja podstawowych narzędzi bezpieczeństwa.
8. Przerwa obiadowa.
9. Zarządzanie wypadkami i incydentami bezpieczeństwa.
10. Szkolenie praktyczne: symulacja reakcji na atak cybernetyczny.
11. Przerwa kawowa.
12. Audyt bezpieczeństwa w placówkach medycznych.
13. Ocena skuteczności środków bezpieczeństwa w kontekście pracy pracowników placówek medycznych.
14. Podsumowanie szkolenia, sesja pytań i odpowiedzi oraz wręczenie certyfikatów.
15. Walidacja efektów uczenia się.

Harmonogram

Liczba przedmiotów/zajęć: 0

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 013,50 PLN
Koszt przypadający na 1 uczestnika netto	2 450,00 PLN
Koszt osobogodziny brutto	188,34 PLN
Koszt osobogodziny netto	153,13 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Krzysztof Musiał

Doświadczony trener , wykładowca, programista, administrator systemów informatycznych. Z wykształcenia absolwent Politechniki Wrocławskiej, Wiceprezes stowarzyszenia przyjaciół rodziców i dzieci z wadą słuchu Orator. Przez wiele lat prowadził liczne szkolenia dla kierowników aptek – dla pojedynczych aptek jak i dużych sieci aptek. Posiada 3 letnie doświadczenie w projektowaniu i tworzeniu zdalnych usług rozwojowych. Zrealizował 10 projektów zdalnej usługi rozwojowej w ostatnich 3 latach głównie dla sektora Ochrony Zdrowia. Posiada 10 letnie doświadczenie w prowadzeniu szkoleń dla lekarzy, menedżerów służby zdrowia w zakresie organizacji pracy w jednostkach i jak i bezpieczeństwa systemów IT w takich jednostkach, ponad 2000 godzin szkoleń. Znajomość na poziomie zaawansowanym narzędzi IT do realizacji usług zdalnych (Zoom, Slack, MS Teams, Google Meet) 2018-2019 - wykładowca na Akademii Sztuki Wojennej w zakresie bezpieczeństwa informacji w jednostkach służby zdrowia. Trener z dużym dorobkiem dydaktycznym i wiedzą merytoryczną.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymują: skrypt szkoleniowy, prezentację multimedialną, indywidualne długopisy, kartki, markery i inne jednorazowe pomoce dydaktyczne a także certyfikat ukończenia szkolenia oraz materiały niezbędne do przeprowadzenia gier/testów/ćwiczeń dydaktycznych podczas szkolenia.

Warunki uczestnictwa

Uczestnik musi być pełnoletni.

Organizator może odwołać szkolenie, jeżeli nie zbierze się minimalna grupa 6 osób.

Informacje dodatkowe

Każdy uczestnik szkolenia zobligowany jest do posiadania laptopa z możliwością korzystania z sieci Wi-Fi, aby mógł wykonywać ćwiczenia praktyczne w grupie i indywidualnie.

Uczestnik po zakończeniu usługi otrzymuje odpowiednie zaświadczenie/certyfikat

W trakcie szkolenia zachowane będą środki ostrożności i bezpieczeństwa uczestników szkolenia.

Realizujemy usługi szkoleniowe również w **formie zamkniętej – dedykowanej**, wówczas program i warunki organizacyjne (termin, miejsce) ustalamy wspólne z Klientem. Pracujemy **stacjonarnie oraz zdalnie**.

Zawarto umowę z WUP w Toruniu w ramach projektu Kierunek – Rozwój.

Dla uczestników z dofinansowaniem min. 70% kwoty szkolenia - stawka „zw" – „§ 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"

Zapraszamy do kontaktu, w celu ustalenia formy szkolenia i sposobu pracy: tel. 508643155 71 lub 71 877 75 25 justyna.wania@activemed.pl

Adres

Gdańsk

Gdańsk

woj. pomorskie

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi

Kontakt

Edyta Budzińska-Musiał

E-mail edyta.bmusial@mbmacademy.pl

Telefon (+48) 519 305 416