Możliwość dofinansowania

Ochrona Danych Medycznych i Cyberbezpieczeństwo w Placówkach Medycznych – Praktyczne Podejście

Numer usługi 2026/04/09/157622/3474968

1 968,00 PLN brutto
1 600,00 PLN netto
246,00 PLN brutto/h
200,00 PLN netto/h
261,33 PLN cena rynkowa

Grupa WW GovTech sp. z o.o.

4,8 / 5

52 oceny

Usługa szkoleniowa
zdalna w czasie rzeczywistym
08:00 h
25.05.2026 do 25.05.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikatory projektów	Kierunek - Rozwój, Nowy start w Małopolsce z EURESEM, Małopolski Pociąg do kariery, Zachodniopomorskie Bony Szkoleniowe
Grupa docelowa usługi	**Grupa docelowa** • Personel medyczny (lekarze, pielęgniarki, rejestratorki, technicy), • Personel administracyjny placówek medycznych, • Właściciele i kierownicy podmiotów leczniczych, • Osoby odpowiedzialne za ochronę danych osobowych i IT w placówkach medycznych, • Wszystkie osoby, które mają kontakt z danymi osobowymi pacjentów. **Usługa również adresowana dla:** • Uczestników projektu Kierunek-Rozwój • Uczestników projektu Bony rozwojowe • Uczestników Projektu MP oraz dla uczestników projektu NSE • Uczestników Projektu "Małopolski pociąg do kariery i/lub dla Uczestników Projektu "Nowy start w Małopolsce z EURESem". • Uczestników innych Projektów
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	21-05-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	8

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

Rozwój kompetencji w zakresie bezpiecznego przetwarzania danych osobowych pacjentów oraz cyberbezpieczeństwa w placówkach medycznych.
Uczestnicy po zakończeniu szkolenia będą:
• rozumieli zasady ochrony danych osobowych zgodne z RODO,
• wskazywali najczęstsze zagrożenia cyberbezpieczeństwa w medycynie,
• wdrażali zabezpieczenia systemów przechowywania danych medycznych (np. NAS, szyfrowanie),
• podejmowali odpowiednie działania w przypadku incydentu naruszenia bezpieczeństwa informacji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik wskazuje zasady ochrony danych medycznych i osobowych wynikające z RODO w działalności placówki medycznej.	Poprawnie identyfikuje obowiązki administratora danych oraz podstawowe wymagania dotyczące ochrony danych medycznych.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik wskazuje metody zabezpieczania danych w placówkach medycznych, w tym szyfrowanie oraz wykorzystanie systemów do bezpiecznego przechowywania danych	Prawidłowo rozróżnia i wskazuje metody zabezpieczeń danych oraz ich zastosowanie.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik rozróżnia najczęstsze zagrożenia cyberbezpieczeństwa w placówkach medycznych oraz wskazuje podstawowe sposoby ich ograniczania.	Poprawnie identyfikuje zagrożenia oraz przyporządkowuje im adekwatne środki ochrony.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik wskazuje zasady tworzenia i utrzymywania kopii zapasowych danych pacjentów oraz rozróżnia podstawowe pojęcia związane z ciągłością działania.	Prawidłowo wskazuje elementy polityki backupu oraz podstawowe zasady odtwarzania danych.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik wskazuje zasady bezpiecznego zarządzania hasłami w zespołach medycznych.	Poprawnie identyfikuje zasady tworzenia, przechowywania i udostępniania haseł zgodnie z polityką bezpieczeństwa.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik wskazuje podstawowe kroki postępowania w przypadku naruszenia bezpieczeństwa informacji w placówce medycznej.	Prawidłowo identyfikuje kolejność działań oraz role odpowiedzialne za reagowanie na incydent.	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Program

Moduł A: Ochrona danych osobowych i medycznych w praktyce

- **Wymagania prawne** dla ochrony danych medycznych: RODO, prawo krajowe.
- **Podstawowe zasady** przechowywania danych medycznych.
- **Bezpieczne procesy** przetwarzania informacji o pacjentach.
- Wprowadzenie do systemów **NAS** w medycynie (różne typy zabezpieczeń).

Moduł B: Cyberbezpieczeństwo w placówkach medycznych

- **Zarządzanie dostępem** i uprawnieniami w systemach medycznych.
- **Bezpieczne przechowywanie danych** – szyfrowanie, kontrola dostępu.
- **Zarządzanie hasłami** w zespołach medycznych: polityki silnych haseł i baza haseł zespołowych.

Moduł C: Reakcja na incydenty i zarządzanie bezpieczeństwem

- **Identyfikacja incydentów** naruszenia bezpieczeństwa.
- **Planowanie działań naprawczych**: jak reagować na wyciek danych, jak dokumentować incydenty.
- **Polityka backupu** danych pacjentów i procedury odzyskiwania.

Moduł D: Cyberhigiena w pracy zespołowej

- **Zasady bezpiecznej pracy** z dokumentacją, urządzeniami i danymi pacjentów.
- **Cyberhigiena w pracy zdalnej** i mobilnej – minimalizacja ryzyk.

Walidacja: test teoretyczny z wynikiem generowanym automatycznie

Metody dydaktyczne

- Wykład z prezentacją,
- Analiza przypadków rzeczywistych w placówkach medycznych,
- Praca na scenariuszach związanych z naruszeniem bezpieczeństwa informacji.

Harmonogram

Liczba pozycji harmonogramu: 0

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

Cennik

Jeżeli korzystasz z dofinansowania w wysokości co najmniej 70% przysługuje Tobie zwolnienie z podatku VAT

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 968,00 PLN
Koszt przypadający na 1 uczestnika netto	1 600,00 PLN
Koszt osobogodziny brutto	246,00 PLN
Koszt osobogodziny netto	200,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

BARTOSZ LEŚNIAK

Specjalista od zabezpieczeń systemów i sieci komputerowych od ponad 20 lat. Konsultant, szkoleniowiec z cyberbezpieczeństwa. Posiadam uprawnienia audytora wewnętrznego normy ISO27001 i ukończoną specjalizację Cyberbezpieczeństwa i Systemów Zarządzania Bezpieczeństwem Informacji na AGH w Krakowie.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymują:

- prezentację ze szkolenia,

- zaświadczenie o ukończeniu szkolenia.

Warunki uczestnictwa

Wymogi unijne związane z realizacją szkolenia z dofinansowaniem:

- Logowanie się pełnym imieniem i nazwiskiem
- Włączona kamera oraz dostęp do mikrofonu

Niespełnienie powyższych może skutkować brakiem dofinansowania

- Warunkiem uzyskania zaświadczenia jest uczestnictwo w co najmniej 80%- 100% (w zależności od programu dofinansowania i podpisanej umowy z Operatorem) zajęć usługi rozwojowej
- W ramach realizacji usług szkoleniowych, Organizator utrwala wizerunek Uczestników w formie nagrań wideo, fotografii lub innych materiałów audiowizualnych wyłącznie w celach archiwizacyjnych, kontrolnych oraz dokumentacyjnych związanych z projektem dofinansowanym.
- Uczestnik zapisując się na szkolenie wyraża zgodę na utrwalenie i wykorzystanie jego wizerunku w wyżej wymienionych celach.
- Organizator nie udostępnia nagrań Uczestnikom po szkoleniu.

Informacje dodatkowe

Zawarto Umowę z UP Toruń w ramach projektu Kierunek Rozwój

Szkolenie prowadzone jest w godzinach dydaktycznych 45 min (8 godzin dydaktycznych = 6 godzin zegarowych)

Przerwy nie są wliczone do czasu usługi.

Podstawa zwolnienia z VAT:

1. art. 43 ust. 1 pkt 29 lit. c ustawy o VAT – dofinansowanie 100%,
2. § 3 ust. 1 pkt 14 rozporządzenia MF – dofinansowanie min. 70%,
3. przy dofinansowaniu poniżej 70% do ceny doliczany jest VAT 23%.

Warunki techniczne

Każdy uczestnik szkolenia powinien mieć możliwość korzystania z komputera z dostępem do Internetu.

Szkolenie będzie się odbywać za pomocą aplikacji Zoom – przed szkoleniem Uczestnicy otrzymają link.

Wymagania techniczne w przypadku szkoleń online:

- Procesor dwurdzeniowy 2GHz lub lepszy (zalecany czterordzeniowy)
- 2 GB pamięci RAM (zalecane 4 GB lub więcej)
- System operacyjny Windows 8 (zalecany Windows 10), Mac OS wersja 10.13 (zalecana najnowsza wersja), Linux, ChromeOS
- Ponieważ szkolenie prowadzone będzie na platformie opartej na przeglądarce, wymagane jest korzystanie z ich najaktualniejszych oficjalnych wersji, takich jak Google Chrome, Mozilla Firefox, Safari, Edge, Opera.
- Będzie to szkolenie realizowane w trybie dyskusji – umożliwi ona uczestnikom rozmowę wideo w czasie rzeczywistym zarówno z prowadzącym, jak też z innymi uczestnikami. Dzięki temu uczestnicy mają wrażenie osobistego udziału w szkoleniu z prowadzącym i innymi uczestnikami.
- Kamera internetowa oraz mikrofon.

Kontakt

ELŻBIETA RACHTAN

E-mail e.rachtan@grupaww.dev
Telefon (+48) 793 123 470