Możliwość dofinansowania

EMM Consulting
Mariusz Lasak

Cyberbezpieczeństwo i cyberhigiena – praktyczne podejście dla kadry i pracowników jednostek medycznych.

Numer usługi 2025/04/17/32347/2695730

zdalna w czasie rzeczywistym
Usługa szkoleniowa
8 h
11.07.2025 do 11.07.2025

2 938,00 PLN brutto
2 938,00 PLN netto
367,25 PLN brutto/h
367,25 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Kadra kierownicza, pracownicy administracyjni i medyczni
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	30
Data zakończenia rekrutacji	10-07-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	8
Podstawa uzyskania wpisu do BUR	Znak Jakości TGLS Quality Alliance

Cel

Cel edukacyjny

Podniesienie kompetencji uczestników w zakresie rozpoznawania zagrożeń cyfrowych, reagowania na incydenty, odpowiedzialności prawnej oraz wdrażania zasad cyberhigieny i bezpieczeństwa informacji w codziennej pracy.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozróżnia podstawowe pojęcia związane z cyberbezpieczeństwem, takie jak malware, phishing, bezpieczne hasła itp.	Uczestnik poprawnie definiuje pojęcia i opisuje ich znaczenie w kontekście bezpieczeństwa sieciowego.	Test teoretyczny z wynikiem generowanym automatycznie
Charakteryzuje różne typy zagrożeń cyfrowych oraz metody ich rozpoznawania.	Uczestnik wymienia i opisuje co najmniej trzy różne typy zagrożeń, podając przykłady oraz sposoby ich identyfikacji.	Test teoretyczny z wynikiem generowanym automatycznie
Stosuje praktyki tworzenia i zarządzania bezpiecznymi hasłami.	Uczestnik demonstruje umiejętność tworzenia silnych haseł i korzystania z menedżerów haseł do ich przechowywania.	Test teoretyczny z wynikiem generowanym automatycznie
Identyfikuje i reaguje na próby phishingu i inne oszustwa internetowe.	Uczestnik poprawnie identyfikuje fałszywe wiadomości e-mail i strony internetowe oraz zna procedury reagowania.	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 zasady bezpiecznego korzystania z sieci publicznych i prywatnych.	Uczestnik potrafi skonfigurować bezpieczne połączenie sieciowe i stosuje praktyki ochrony prywatności.	Test teoretyczny z wynikiem generowanym automatycznie
Wskazuje podstawy prawne ochrony danych osobowych i cyberbezpieczeństwa.	Uczestnik rozróżnia podstawy prawne na poziomie międzynarodowym, unijnym i krajowym oraz interpretuje przepisy prawa.	Test teoretyczny z wynikiem generowanym automatycznie
Wykonuje kopie zapasowe plików i danych.	Uczestnik rozróżnia metody tworzenia kopii zapasowej, charakteryzuje zasady ich tworzenia i organizuje proces backupu.	Test teoretyczny z wynikiem generowanym automatycznie
Włącza opcję dwuskładnikowej autoryzacji w mediach społecznościowych.	Uczestnik demonstruje, w jaki sposób włącza opcję 2FA i uzasadnia jej istotę.	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?

Certyfikat 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?

Walidacja została przeprowadzona w oparciu o zdefiniowane efekty uczenia się.

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

Trener kursu rozwiązując w czasie rzeczywistym zadania w MS Excel reaguje na bieżąco na efekt w postaci wzrostu poziomu wiedzy. Kształcenie oraz badanie efektów oraz walidacja prowadzone przez różne osoby.

Program

1. Wprowadzenie do cyberbezpieczeństwa i cyberhigieny

- Co to jest cyberbezpieczeństwo i dlaczego dotyczy każdego?

- Wspólna odpowiedzialność – kadra i pracownicy

- Przykłady realnych incydentów w administracji i ochronie zdrowia

2. Obowiązujące podstawy prawne

- Ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC)

- RODO w kontekście bezpieczeństwa danych

- Odpowiedzialność kadry i pracowników za naruszenia

- Wewnętrzne procedury bezpieczeństwa – dlaczego są ważne?

3. Typy cyberataków i przykłady

- Phishing, ransomware, socjotechnika, ataki na konta

- Jak wyglądają ataki "od kuchni" – studia przypadków

- Ataki na placówki medyczne i JST – lekcje z incydentów

4. Zasady cyberhigieny w codziennej pracy

- Hasła, loginy, uwierzytelnianie dwuskładnikowe

- Zasady bezpiecznego korzystania z poczty i Internetu

- Praca zdalna i mobilna – ryzyka i dobre praktyki

- Ochrona danych pacjentów / interesantów

5. Reagowanie na incydenty

- Czym jest incydent i jak go rozpoznać?

- Procedury zgłaszania – kogo poinformować i kiedy?

- Rola kadry kierowniczej i pracowników w sytuacji kryzysowej

- Tworzenie kultury szybkiego reagowania

6. Testowanie i audyt bezpieczeństwa

- Testy penetracyjne i analiza podatności – podstawowe informacje

- Samodzielna ocena ryzyk i zagrożeń

- Współpraca z zespołami IT i ABI/IOD

7. Rola kadry zarządzającej w budowie odporności cyfrowej

- Strategiczne podejście do bezpieczeństwa informacji

- Kształtowanie polityki bezpieczeństwa

- Budowanie świadomości w zespole

8. Podsumowanie i ewaluacja

- Quiz sprawdzający wiedzę uczestników

- Wspólne omówienie typowych błędów i sposobów ich unikania

- Wręczenie certyfikatów ukończenia szkolenia (opcjonalnie)

Harmonogram

Liczba przedmiotów/zajęć: 7

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 7 Wprowadzenie do cyberbezpieczeństwa i cyberhigieny Obowiązujące podstawy prawne Typy cyberataków i przykłady	Adam Pistelok	11-07-2025	08:00	09:30	01:30
2 z 7 walidacja	-	11-07-2025	09:30	09:45	00:15
3 z 7 Zasady cyberhigieny w codziennej pracy Reagowanie na incydenty Testowanie i audyt bezpieczeństwa	Adam Pistelok	11-07-2025	09:45	11:15	01:30
4 z 7 walidacja	-	11-07-2025	11:15	11:30	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 7 Rola kadry zarządzającej w budowie odporności cyfrowej	Adam Pistelok	11-07-2025	11:30	13:00	01:30
6 z 7 walidacja	-	11-07-2025	13:00	13:15	00:15
7 z 7 Podsumowanie i prezentacja przykładów	Adam Pistelok	11-07-2025	13:15	15:00	01:45

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 938,00 PLN
Koszt przypadający na 1 uczestnika netto	2 938,00 PLN
Koszt osobogodziny brutto	367,25 PLN
Koszt osobogodziny netto	367,25 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Adam Pistelok

doświadczony trener i ekspert w zakresie nowych technologii, ceniony przede wszystkim za swoje wyjątkowe kompetencje w dziedzinie Excela, cyberbezpieczeństwa i szeroko rozumianych kompetencji cyfrowych. Przez ostatnie 5 lat przeszkolił ponad 1500 osób, realizując dziesiątki tysięcy godzin szkoleń zarówno stacjonarnie, jak i online.

Jako certyfikowany egzaminator ECDL Advanced, DigComp oraz ECCC, posiada nie tylko szeroką wiedzę teoretyczną, ale przede wszystkim potrafi skutecznie przekładać ją na praktyczne umiejętności przydatne w pracy biurowej, administracyjnej i medycznej.

Prowadził wiele szkoleń z zakresu cyberbezpieczeństwa, ochrony danych osobowych i cyberhigieny, w tym także dla pracowników jednostek medycznych, samorządów oraz administracji publicznej.

Jego zajęcia są wysoko oceniane za klarowność przekazu, interaktywność oraz indywidualne podejście do uczestników.

Prowadzi zarówno szkolenia grupowe, jak i indywidualne – pracując z osobami aktywnymi zawodowo, osobami bezrobotnymi, seniorami, a także osobami z niepełnosprawnościami. Znany z wysokiego poziomu empatii i komunikatywności, potrafi stworzyć komfortową i bezpieczną atmosferę do nauki, co szczególnie cenią uczestnicy jego kursów.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały dla uczestników

- Skrypt szkoleniowy (PDF)

- Lista kontrolna cyberhigieny do zastosowania w miejscu pracy

- Przykładowe scenariusze incydentów i schematy reakcji

- Wzorcowa polityka bezpieczeństwa informacji (do adaptacji)

Warunki uczestnictwa

Warunki uczestnictwa

- Warunkiem ukończenia kursu jest frekwencja na poziomie co najmniej 80% zajęć.
- Uczestnik zgadza się na utrwalania jego wizerunku na potrzeby monitoringu/kontroli instytucji finansującej kurs.

Warunki techniczne

Wymagania sprzętowe:

- Procesor dwurdzeniowy 2GHz lub lepszy (zalecany czterordzeniowy);
- 2GB pamięci RAM (zalecane 4GB lub więcej);
- System operacyjny taki jak Windows 8 (zalecany Windows 11), Mac OS wersja 10.13 (zalecana najnowsza wersja), Linux, Chrome OS.

Wymagania dotyczące łącza internetowego:

https://knowledge.clickmeeting.com/pl/knowledge-base/pierwsze-kroki/o-clickmeeting/#jakiego-lacza-potrzebuje-aby-moc-korzystac-z-platformy-clickmeeting

Osoby korzystające z aplikacji Clickmeeting mogą skorzystać z poradnika. Dostępnego pod niniejszym linkiem:

https://knowledge.clickmeeting.com/uploads/2022/05/Poko%CC%81j_webinarowy_wskazo%CC%81wki_dla-uczestniko%CC%81w.pdf

Filmy instruujące jak dołączyć do wydarzeń Clickmeeting:

1. Bez rejestracji: https://knowledge.clickmeeting.com/pl/video-tutorials/jak-dolaczyc
2. Z rejestracją: https://knowledge.clickmeeting.com/pl/video-tutorials/jak-dolaczyc-i-sie-zarejestrowac/

Każda z osób zgłoszonych na szkolenie zostanie poinstruowana jak zainstalować niezbędne oprogramowanie (darmowe dla uczestników szkolenia), oraz skonfigurować sprzęt komputerowy, oraz go przetestować.

Kontakt

Mariusz Lasak

E-mail lasakmariusz@gmail.com
Telefon (+48) 502 096 967