

POLSKIE
CENTRUM
AUDYTU**Bezpieczeństwo informacji, danych
osobowych i cyberbezpieczeństwo w
placówce medycznej**

Numer usługi 2025/12/22/40606/3226802

4 998,00 PLN brutto
4 998,00 PLN netto
294,00 PLN brutto/h
294,00 PLN netto/h

Górny Karol Speed
Com

★★★★★ 5,0 / 5

182 oceny

📍 Turka / stacjonarna

🏠 Usługa szkoleniowa

🕒 17 h

📅 31.01.2026 do 03.02.2026

Informacje podstawowe

Kategoria	Prawo i administracja / Prawo pozostałe
Grupa docelowa usługi	Personel medyczny (lekarze, pielęgniarki, rejestratorki), personel administracyjny placówek medycznych, właściciele i kierownicy podmiotów leczniczych, osoby odpowiedzialne za ochronę danych osobowych i IT w placówkach medycznych
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	30-01-2026
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	17
Podstawa uzyskania wpisu do BUR	Standard Usług Szkoleniowo– Rozwojowych PIFS SUS 3.0

Cel

Cel edukacyjny

Po odbytych szkoleniu uczestnicy zdobędą wiedzę, umiejętności oraz kompetencji społeczne niezbędne do bezpiecznego przetwarzania danych medycznych i osobowych w placówce medycznej, zgodnie z wymaganiami RODO oraz zasadami cyberbezpieczeństwa. Będą przygotowani do samodzielnego wdrażania zabezpieczeń technicznych, organizacyjnych oraz reagowania na incydenty bezpieczeństwa informacji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wymienia podstawy prawne przetwarzania danych medycznych i osobowych, w tym wymagania RODO	Poprawnie identyfikuje obowiązki administratora danych oraz sytuacje naruszeń	Test teoretyczny
Wymienia zasady bezpiecznego przechowywania i szyfrowania danych medycznych	Poprawnie wskazuje metody zabezpieczeń i ich zastosowanie	Test teoretyczny
Wymienia zagrożenia cyberbezpieczeństwa w placówkach medycznych	Prawidłowo rozpoznaje rodzaje zagrożeń w opisanych przypadkach	Test teoretyczny
Konfiguruje podstawowe zabezpieczenia systemu przechowywania danych (NAS)	Poprawnie wykonuje konfigurację szyfrowania i kontroli dostępu	Prezentacja
Planuje i wdraża politykę kopii zapasowych danych pacjentów	Prawidłowo tworzy harmonogram backupu i procedurę odtwarzania	Prezentacja
Stosuje bezpieczne metody zarządzania hasłami zespołowymi	Poprawnie tworzy i zarządza bazą haseł zgodnie z polityką bezpieczeństwa	Obserwacja w warunkach symulowanych
Reaguje na incydent naruszenia bezpieczeństwa informacji	Poprawnie opisuje i planuje działania naprawcze	Obserwacja w warunkach symulowanych
Stosuje zasady cyberhigieny w pracy zespołowej	Konsekwentnie przestrzega ustalonych procedur	Obserwacja w warunkach symulowanych
Podejmuje odpowiedzialne decyzje w sytuacjach zagrożenia bezpieczeństwa informacji	Właściwie dobiera działania w sytuacjach problemowych	Analiza dowodów i deklaracji

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

Dzień 1

- Przywitanie i wypełnienie pre testu

MODUŁ 1: Bezpieczne Przechowywanie Danych Medycznych

1.Wprowadzenie do systemów NAS w medycynie

- Wymagania prawne dla danych medycznych
- Standardy bezpieczeństwa RODO/ISO 27001
- Architektura systemu Synology DS423

2. Konfiguracja zabezpieczeń

- Szyfrowanie dysków i folderów
- Konfiguracja użytkowników i grup
- Ustawienia zapory sieciowej

3. Systemy backup i recovery

- Automatyczne kopie zapasowe
- Testowanie procedur odzyskiwania
- Dokumentacja incydentów

Dzień 2

MODUŁ 2: Cyberbezpieczeństwo w medycynie

1. Sejf haseł (secure vault)

- Tworzenie bazy haseł zespołowych
- Polityki silnych haseł
- Udostępnianie bezpieczne

2. Monitoring bezpieczeństwa

- Logi dostępu i aktywności
- Wykrywanie anomalii
- Procedury reagowania na incydenty

3. Compliance medyczny

- Audyty zgodności z RODO
- Dokumentacja procesów
- Raportowanie naruszeń
- Test wiedzy po szkoleniu

-Wypełnienie ankiety ewaluacyjnej, rozdanie zaświadczeń, pożegnanie

Szkolenie trwa 17 godzin dydaktycznych. Godzina dydaktyczna to 45 minut, (czyli 12 godzin i 45 minut zegarowych). W każdym dniu szkolenia uwzględniona została przerwa minimum półgodzinna, która jest wliczona w czas szkolenia.

Na część teoretyczną, ewaluacyjną i walidacyjną przeznaczone jest 2,5 godziny zegarowe, pozostały czas to praca warsztatowa uwzględniająca przerwy.

Materiały szkoleniowe zostaną przekazane uczestnikom w formie prezentacji oraz przykładowych wzorów dokumentów z zakresu ochrony danych osobowych.

W szkoleniu mogą również uczestniczyć wszystkie osoby, niezależnie od poziomu wiedzy z zakresu bezpieczeństwo informacji, danych osobowych i cyberbezpieczeństwo w placówce medycznej

Szkolenie zakończone zostanie wypełnieniem post testu oraz ankiet ewaluacyjnych oraz rozdaniem zaświadczeń potwierdzających nabyte kompetencje i ukończenie szkolenia.

Warunkiem ukończenia szkolenia jest frekwencja na poziomie 80 %.

Przed rozpoczęciem szkolenia przeprowadzony zostanie wstępny test wiedzy uczestników. Po ostatnim dniu szkolenia ten sam test wiedzy zostanie powtórzony celem sprawdzenia efektów szkolenia. Test będzie miał formę pytań zamkniętych wielokrotnego wyboru i będzie obejmował co najmniej jedno pytanie z każdego obszaru tematycznego uwzględnionego w harmonogramie szkolenia.

Osoba walidująca waliduje usługę po jej zakończeniu, w oparciu o checklistę od trenera.

Harmonogram

Liczba przedmiotów/zajęć: 23

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 23 Przywitanie i wypełnienie pre testu	Hubert Puacz	31-01-2026	09:00	09:30	00:30
2 z 23 Wymagania prawne dla danych medycznych	Hubert Puacz	31-01-2026	09:30	10:00	00:30
3 z 23 Standardy bezpieczeństwa RODO/ISO 27001	Hubert Puacz	31-01-2026	10:00	10:30	00:30
4 z 23 Architektura systemu Synology DS423	Hubert Puacz	31-01-2026	10:30	11:20	00:50
5 z 23 Przerwa	Hubert Puacz	31-01-2026	11:20	11:50	00:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
6 z 23 Szyfrowanie dysków i folderów	Hubert Puacz	31-01-2026	11:50	12:30	00:40
7 z 23 Konfiguracja użytkowników i grup	Hubert Puacz	31-01-2026	12:30	13:20	00:50
8 z 23 Ustawienia zapory sieciowej	Hubert Puacz	31-01-2026	13:20	14:00	00:40
9 z 23 Automatyczne kopie zapasowe	Hubert Puacz	31-01-2026	14:00	14:45	00:45
10 z 23 Testowanie procedur odzyskiwania	Hubert Puacz	31-01-2026	14:45	15:00	00:15
11 z 23 Dokumentacja incydentów	Hubert Puacz	31-01-2026	15:00	15:45	00:45
12 z 23 Tworzenie bazy haseł zespołowych	Hubert Puacz	03-02-2026	09:00	09:40	00:40
13 z 23 Polityki silnych haseł	Hubert Puacz	03-02-2026	09:40	10:20	00:40
14 z 23 Udostępnianie bezpieczne	Hubert Puacz	03-02-2026	10:20	11:00	00:40
15 z 23 Logi dostępu i aktywności	Hubert Puacz	03-02-2026	11:00	11:30	00:30
16 z 23 Wykrywanie anomalii	Hubert Puacz	03-02-2026	11:30	12:00	00:30
17 z 23 Procedury reagowania na incydenty	Hubert Puacz	03-02-2026	12:00	12:30	00:30
18 z 23 Przerwa	Hubert Puacz	03-02-2026	12:30	13:00	00:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
19 z 23 Audyty zgodności z RODO	Hubert Puacz	03-02-2026	13:00	13:30	00:30
20 z 23 Dokumentacja procesów	Hubert Puacz	03-02-2026	13:30	14:00	00:30
21 z 23 Raportowanie naruszeń	Hubert Puacz	03-02-2026	14:00	14:20	00:20
22 z 23 Test wiedzy po szkoleniu	-	03-02-2026	14:20	14:40	00:20
23 z 23 Wypełnienie ankiety ewaluacyjnej, rozdanie zaświadczeń, pożegnanie	Hubert Puacz	03-02-2026	14:40	15:00	00:20

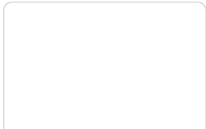
Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 998,00 PLN
Koszt przypadający na 1 uczestnika netto	4 998,00 PLN
Koszt osobogodziny brutto	294,00 PLN
Koszt osobogodziny netto	294,00 PLN

Prowadzący

Liczba prowadzących: 2



1 z 2
Karol Górny



Ekspert w dziedzinie ochrony danych osobowych i bezpieczeństwa informacji

Doświadczony praktyk specjalizujący się w ochronie danych osobowych, audytach bezpieczeństwa informacji oraz praktycznym wdrażaniu RODO w różnych typach organizacji. Założyciel Polskiego Centrum Audytu, pełniący funkcję Audytora Wiodącego Systemów Zarządzania Bezpieczeństwem Informacji zgodnie z normą PN-EN ISO/IEC 27001:2023-08.

Absolwent kierunków Administracja oraz Ochrona Danych Osobowych na Uniwersytecie Marii Curie-Skłodowskiej w Lublinie. Od lat sprawuje funkcję Inspektora Ochrony Danych w podmiotach sektora publicznego i prywatnego, w tym w jednostkach administracji samorządowej, instytucjach edukacyjnych, firmach produkcyjnych oraz organizacjach pozarządowych.

Specjalizuje się w szkoleniach opartych na realnych przypadkach, analizie incydentów oraz interpretacji przepisów prawa z uwzględnieniem ich praktycznego zastosowania w codziennej działalności organizacji. Łączy podejście systemowe, wynikające z praktyki audytorskiej, z warsztatowym przekazem wiedzy. W swoich programach rozwija autorskie metody wdrożeniowe, w tym m.in. skuteczne modele mapowania procesów przetwarzania danych, oceny ryzyka oraz zarządzania dokumentacją ochrony danych osobowych



2 z 2

Hubert Puacz

Konsultant, architekt systemów teleinformatycznych, projektuje rozwiązania infrastruktury sieciowej w chmurze i on-premise dla klientów z branży farmaceutycznej, finansowej, bankowej oraz innych. Zajmuję się wdrażaniem, konfiguracją, aktualizacją i administracją sieci, urządzeń, szeroko pojętego zabezpieczania, monitorowania i kontroli dostępu (role, użytkownicy), wdrażania procesów backup/disaster recovery zgodnych z RODO. W trakcie studiów na Wojskowej Akademii Technicznej w Warszawie 2009-2014 kształcił się w zakresie sieci i bezpieczeństwa systemów teleinformatycznych. Po ukończeniu studiów pracował jako programista, a później jako DevOps, łącząc to jednocześnie z prowadzeniem działalności gospodarczej realizującej usługi hostingowe, tworzenia stron www i wdrażania rozwiązań dla sieci lokalnych (np. montażu i instalacji WiFi mesh, routingu czy warstwy składowania danych NAS Synology/Qnap). Od 11 lat prowadzi działalność związaną z tematyką sieciową, bezpieczeństwa sieciowego, hostingu i tworzenia stron www. Od początku prowadzenia działalności szkoli klientów w zakresie używania wdrożonych rozwiązań. Od 2023 występuje publicznie i dzieli się zdobytą wiedzą na konferencjach i spotkaniach grup technologicznych.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały szkoleniowe zostaną przekazane uczestnikom w formie prezentacji oraz przykładowych wzorów dokumentów z zakresu ochrony danych osobowych.

Warunki uczestnictwa

Warunkiem uczestnictwa jest prawidłowy zapis na usługę w BUR

Informacje dodatkowe

Usługa jest zwolniona z podatku Vat w przypadku dofinansowania na minimalnym poziomie 70%.

Zwolnienie podatkowe dla usług szkoleniowych sfinansowany ze środków publicznych co najmniej w 70% (art. 43 ust. 1 pkt 29 lit. c iust. 17a ustawy o VAT oraz § 3 ust. 1 pkt 14 i ust. 8-9 rozporządzenia Ministra Finansów z 20.12.2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień).

Adres

ul. Klonowa 33
20-258 Turka
woj. lubelskie

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi

Kontakt



Karol Górny

E-mail k.gorny@pcat.pl

Telefon (+48) 605 300 663