

Specjalista ds. SZBI

📍 Warszawa

Link do oferty: <https://jobtime.pl/praca/4863014/specjalista-ds-szbi>

📄 Pracodawca

NARODOWY INSTYTUT KARDIOLOGII STEFANA KARDYNAŁA WYSZYŃSKIEGO - PAŃSTWOWY INSTYTUT BADAWCZY

Warszawa

📄 Wynagrodzenie

UoP: 10 000 - 16 000 PLN

📄 Szczegóły oferty

Forma zatrudnienia	Umowa o pracę
Wymiar pracy	Pełny etat
Data publikacji	09.06.2026
Ważna do	09.07.2026

📄 Oferujemy

Specjalista / Starszy Specjalista ds. SZBI

Wynagrodzenie: 10 000-16 000 zł brutto

Forma zatrudnienia: umowa o pracę

Miejsce pracy: Warszawa, Anin

Tryb pracy: praca stacjonarna z możliwością pracy hybrydowej

Poziom stanowiska: Specjalista / Starszy Specjalista — w zależności od doświadczenia i samodzielności

Ważne: w treści aplikacji lub wiadomości do rekrutera prosimy o podanie sugerowanego / oczekiwanego wynagrodzenia brutto.

W związku z rozwojem Działu Systemów Informatycznych i Cyberbezpieczeństwa oraz dalszym doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji poszukujemy osoby na stanowisko:

Specjalista / Starszy Specjalista ds. SZBI

Osoba zatrudniona na tym stanowisku będzie odpowiedzialna za utrzymanie, aktualizację i rozwój dokumentacji SZBI, nadzór nad rejestrami, udział w analizie ryzyka, przygotowywanie audytów wewnętrznych oraz wspieranie organizacji w utrzymaniu zgodności z wymaganiami ISO/IEC 27001, ISO 22301, ustawy o krajowym systemie cyberbezpieczeństwa oraz innych przepisów dotyczących

bezpieczeństwa informacji, cyberbezpieczeństwa, ochrony danych i ciągłości działania.

Minimalne wymagania

- wykształcenie wyższe
- doświadczenie w obszarze SZBI, bezpieczeństwa informacji, audytów wewnętrznych, analizy ryzyka, compliance lub systemów zarządzania
- certyfikat audytora wewnętrznego ISO/IEC 27001
- znajomość ISO/IEC 27001, ISO 22301, ustawy o krajowym systemie cyberbezpieczeństwa oraz podstawowych wymagań prawnych dotyczących bezpieczeństwa informacji, ochrony danych i ciągłości działania

Główny zakres zadań

- utrzymanie, aktualizacja i rozwój dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji
- przegląd i aktualizacja polityk, procedur, instrukcji, formularzy, rejestrów i raportów SZBI
- nadzór nad aktualnością rejestrów związanych z bezpieczeństwem informacji
- prowadzenie lub współprowadzenie rejestru ryzyk, aktywów, incydentów, działań korygujących, dostawców, systemów i procesów
- udział w analizie ryzyka dla systemów, procesów, aktywów informacyjnych, dostawców i obszarów organizacyjnych
- wsparcie właścicieli procesów i właścicieli aktywów w identyfikacji ryzyk, zabezpieczeń oraz działań ograniczających ryzyko
- przygotowywanie, prowadzenie i dokumentowanie audytów wewnętrznych zgodnie z ISO/IEC 27001 i ISO 22301
- opracowywanie raportów z audytów, niezgodności, obserwacji, rekomendacji oraz działań korygujących
- monitorowanie realizacji działań poaudytowych, korygujących i doskonalących
- udział w przygotowywaniu materiałów do audytów, kontroli, przeglądów zarządzania i ocen zgodności
- monitorowanie zmian w wymaganiach prawnych, regulacyjnych i normatywnych dotyczących bezpieczeństwa informacji, cyberbezpieczeństwa i ciągłości działania
- udział w dostosowywaniu dokumentacji SZBI do ustawy o krajowym systemie cyberbezpieczeństwa, RODO, wymagań sektorowych i innych regulacji właściwych dla Instytutu
- wspieranie procesu zarządzania incydentami bezpieczeństwa informacji od strony dokumentacyjnej, rejestrowej i analitycznej
- wspieranie nadzoru nad dostawcami w zakresie bezpieczeństwa informacji, dostępu, ciągłości działania i zgodności z wymaganiami wewnętrznymi
- udział w opiniowaniu dokumentów, procedur, wymagań i zapisów dotyczących bezpieczeństwa informacji w projektach, umowach i postępowaniach zakupowych
- przygotowywanie zestawień, raportów, analiz, notatek i informacji zarządczych dotyczących SZBI, ryzyk, audytów i działań doskonalących
- współpraca z zespołem cyberbezpieczeństwa, administratorami systemów, DPO/IOD, działem prawnym, zamówieniami publicznymi, właścicielami procesów oraz komórkami merytorycznymi

Wymagania

- praktyczna znajomość zasad funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji
- doświadczenie w tworzeniu, aktualizacji lub utrzymaniu dokumentacji SZBI
- znajomość wymagań ISO/IEC 27001
- znajomość wymagań ISO 22301 w zakresie ciągłości działania
- znajomość ustawy o krajowym systemie cyberbezpieczeństwa
- znajomość podstaw RODO oraz zasad ochrony danych osobowych
- znajomość zasad analizy ryzyka

- umiejętność pracy z rejestrami, tabelami, matrycami, zestawieniami i raportami
- umiejętność prowadzenia audytów wewnętrznych i dokumentowania ich wyników
- umiejętność formułowania rekomendacji, działań korygujących i działań doskonalących
- bardzo dobra znajomość pakietu Microsoft Office, w szczególności Word i Excel
- umiejętność redagowania dokumentów formalnych, procedur, notatek, raportów i zaleceń
- dokładność, systematyczność, samodzielność, odpowiedzialność i terminowość
- umiejętność prowadzenia kilku spraw równolegle
- komunikatywność i umiejętność współpracy z osobami technicznymi, administracyjnymi, prawnymi, medycznymi i zarządczymi
- znajomość języka angielskiego w stopniu umożliwiającym korzystanie z dokumentacji normatywnej, technicznej i branżowej

Mile widziane

- certyfikat lub ukończone szkolenie audytora wewnętrznego ISO 22301
- znajomość ISO/IEC 27002, ISO 19011, ISO 31000
- znajomość NIS2, RODO, ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne lub innych regulacji dotyczących cyberbezpieczeństwa i bezpieczeństwa informacji
- doświadczenie w jednostce ochrony zdrowia, instytucie badawczym, administracji publicznej, jednostce publicznej lub dużej organizacji
- doświadczenie w przygotowywaniu organizacji do audytów certyfikacyjnych, nadzoru, recertyfikacji, kontroli lub przeglądów zgodności
- doświadczenie w prowadzeniu rejestru ryzyk, aktywów, incydentów, dostawców, działań korygujących lub innych rejestrów systemowych
- doświadczenie w analizie ryzyka dla systemów informatycznych, procesów organizacyjnych, dostawców lub usług krytycznych
- znajomość zagadnień ciągłości działania, planów awaryjnych, planów odtworzeniowych i testów ciągłości działania
- podstawowa znajomość środowiska IT, systemów informatycznych, infrastruktury, uprawnień, kopii zapasowych, incydentów i usług IT
- doświadczenie w pracy z elektronicznym obiegiem dokumentów, repozytoriami dokumentacji lub narzędziami GRC

Oferujemy

- stabilne zatrudnienie w instytucji naukowej o ugruntowanej pozycji w kraju
- pracę w Dziale Systemów Informatycznych i Cyberbezpieczeństwa
- realny wpływ na rozwój i doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji
- udział w utrzymaniu i rozwoju dokumentacji SZBI, analizie ryzyka, audytach wewnętrznych i przeglądach zgodności
- pracę przy zagadnieniach związanych z ISO/IEC 27001, ISO 22301, ustawą o krajowym systemie cyberbezpieczeństwa, bezpieczeństwem informacji, ciągłością działania i zarządzaniem ryzykiem
- udział w projektach modernizacyjnych, wdrożeniowych i rozwojowych dotyczących cyberbezpieczeństwa, systemów informatycznych i ciągłości działania
- możliwość udziału w dodatkowo płatnych projektach wdrożeniowych, modernizacyjnych i rozwojowych, zgodnie z potrzebami Instytutu, zasadami finansowania projektów oraz decyzjami pracodawcy
- możliwość rozwoju zawodowego, udziału w szkoleniach oraz zdobywania doświadczenia w dużym i złożonym środowisku ochrony zdrowia
- współpracę z administratorami systemów, zespołem cyberbezpieczeństwa, DPO/IOD, działem prawnym, zamówieniami publicznymi, właścicielami procesów i komórkami merytorycznymi

- możliwość pracy hybrydowej w zależności od charakteru zadań, poziomu samodzielności, organizacji pracy oraz potrzeb operacyjnych Instytutu
- pracę od zaraz
- zatrudnienie w oparciu o umowę o pracę
- pracę w Dziale Systemów Informatycznych i Cyberbezpieczeństwa zlokalizowanym poza budynkiem szpitalnym, na oddzielnym, dedykowanym piętrze

Proces rekrutacji

- złożenie aplikacji w systemie elektronicznym Narodowego Instytutu Kardiologii
- wstępna analiza aplikacji i wybór potencjalnych Kandydatów
- rozmowa kwalifikacyjna on-line lub stacjonarna
- możliwość przeprowadzenia dodatkowej rozmowy merytorycznej lub zadania praktycznego
- decyzja o podjęciu współpracy

Zastrzegamy sobie prawo do kontaktu z wybranymi Kandydatami oraz do przeprowadzenia dodatkowego etapu rekrutacji, jeżeli będzie to uzasadnione charakterem stanowiska.

Benefity

Dofinansowanie szkoleń / kursów

Praca zdalna / hybrydowa

 **APLIKUJ TERAZ**

<https://jobtime.pl/praca/4863014/specjalista-ds-szbi#sec5>

Wygenerowano: 2026-06-09 10:22 | JobTime.pl - Portal pracy IT i nie tylko

Oferta może ulec zmianie. Aktualne informacje znajdziesz na stronie: <https://jobtime.pl/praca/4863014/specjalista-ds-szbi>