

Polityka Bezpieczeństwa Informacji i Ochrony Danych Osobowych Zespołu Opieki Zdrowotnej w Końskich

1. Deklaracja

Dyrekcja Zespołu Opieki Zdrowotnej w Końskich potwierdza, że Polityka Bezpieczeństwa i Ochrony Danych Osobowych to zbiór działań, zmierzających do uzyskania i utrzymania adekwatnego poziomu bezpieczeństwa w zakresie przetwarzania danych osobowych w tym danych osobowych szczególnej kategorii. Powyższe realizowane jest poprzez zapewnienia poufności, integralności i dostępności na każdym etapie przetwarzania danych osobowych. Działania te realizowane są z uwzględnieniem zobowiązań ustawowych ze szczególnym uwzględnieniem dobra pacjenta oraz jego praw.

Polityka Bezpieczeństwa i Ochrony Danych Osobowych oraz Instrukcja zarządzania systemem informatycznym zapewnia:

- spójność z wyznaczonymi zadaniami ZOZ,
- integrację z procedurami obowiązującymi w ZOZ w Końskich,
- skuteczniejsze działania w odniesieniu do zagrożeń poufności, integralności i dostępności danych osobowych, w taki sposób, aby podnieść jakość i wiarygodność wobec pacjentów oraz stron zainteresowanych,

Dyrekcja Zespołu Opieki Zdrowotnej w Końskich dokłada wszelkich starań, aby wdrożyć wszelkie niezbędne mechanizmy bezpieczeństwa, aby zrealizować te cele, adekwatnie do rezultatów procesu oceny ryzyka.

2. Dokumentacja

Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji i Ochrony Danych Osobowych w którego skład wchodzi Polityka Bezpieczeństwa i Ochrony Danych Osobowych wraz z deklaracją stosowania stanowi repozytorium udokumentowanej informacji, zawierające dokumentację wymaganą przez normy ISO/IEC 27001:2013 oraz ISO/IEC 19134:2017.

Dokumentacja ta zawiera niezbędne informacje w zakresie bezpieczeństwa informacji i ochrony danych osobowych.

Integralną częścią Polityki są:

- Instrukcja Zarządzania Systemem
- Regulamin przetwarzania danych osobowych
- Wykaz zbiorów danych osobowych
- Ewidencja osób upoważnionych – dostępny u Inspektora Ochrony Danych
- Rejestr czynności przetwarzania – dostępny u Inspektora Ochrony Danych
- Polityka kluczy

Administratorem repozytorium udokumentowanej informacji jest Inspektor Ochrony Danych. Dokumentacja dostępna jest dla wszystkich pracowników oraz stron zainteresowanych w zakresie niezbędnym do wykonywania powierzonych obowiązków służbowych lub do realizacji poprawnego wykonywania umów.

Wszelkie zmiany dokumentacji w tym przegląd i aktualizacja przeprowadzane są przez Inspektora Ochrony Danych

2. Kontekst organizacji

System Zarządzania Bezpieczeństwem Informacji i Ochrony Danych Osobowych został opracowany z uwzględnieniem wymagań prawnych, stron zainteresowanych jak również mając na uwadze aspekty działalności Zespołu Opieki Zdrowotnej w Końskich.

3. Zakres Polityki Bezpieczeństwa i Ochrony Danych Osobowych

Niniejszy dokument określa:

- Zasady bezpieczeństwa przetwarzania danych osobowych, jakie powinny być przestrzegane i stosowane w Zespole Opieki Zdrowotnej w Końskich przez pracowników i strony zewnętrzne, którzy przetwarzają dane osobowe.
- Stosowanie zasad mających na celu zapewnienie prawidłowej ochrony danych osobowych przetwarzanych przez Zespół Opieki Zdrowotnej w Końskich,
- Zasady zarządzania aktywami, zgodnie z obowiązującymi przepisami zewnętrznymi i wewnętrznymi dotyczącymi bezpieczeństwa zasobów informatycznych w tym infrastruktury techniczno-systemowej,
- Zasady dotyczące bezpieczeństwa danych osobowych, ustalonych w oparciu o wymagania wynikające z przepisów prawa, z szacowania ryzyka w związku z określonych kontekstem organizacji.

4. Cele bezpieczeństwa i ochrony danych osobowych

- Zapewnienie bezpieczeństwa przetwarzanym informacjom,
- Zapewnienie bezpieczeństwa danym osobowym w tym danym szczególnie chronionym,
- Zgodność działalności ZOZ w Końskich z wymaganiami prawa, regulatorów i zainteresowanych stron.
- Zapewnienie pozytywnego wizerunku Szpitalowi.

Cele niniejszej Polityki realizowane są przez:

- Zapewnienie poufności oraz utrzymanie integralności i dostępności informacji, w tym danym osobowych oraz infrastruktury wspierającej ich przetwarzanie, w szczególności:
 - danych osobowych pacjentów i personelu medycznego,
 - dokumentacji medycznej pacjentów,

- recept, skierowań, zwolnień lekarskich i zleceń medycznych,
 - rejestrów prowadzonych w ZOZ w Końskich,
 - zapewnienie właściwych mechanizmów autoryzacji użytkowników,
- Zapewnienie bezzwłocznej reakcji na incydenty zagrażające bezpieczeństwu danych osobowych.

6. Zasoby organizacji, odpowiedzialności i role, komunikacja

Dyrektor Szpitala wraz z Inspektorem Ochrony Danych jest bezpośrednio odpowiedzialny za wdrożenie niniejszej Polityki oraz zapewnienia jej przestrzegania przez podległych pracowników.

W celu realizacji zobowiązań *Dyrektor ZOZ w Końskich będący Administratorem Danych Osobowych* powołuje:

- Inspektor Ochrony Danych (IOD) (oraz jego zastępcę), który odpowiada za zapewnienie przez ZOZ w Końskich zgodności przetwarzania danych osobowych z obowiązującym prawem,
- Administratora Sieci Komputerowej (ASK) – Zastępcę Kierownika DSUiZP (Działu Sprzedaży Usług i Zamówień Publicznych) ds. sekcji informatycznej , odpowiedzialnego za utrzymanie i eksploatację systemów teleinformatycznych Szpitala,
- Administratorów Systemów Informatycznych (ASI) – osoby bezpośrednio odpowiedzialne za prawidłowe funkcjonowanie systemów teleinformatycznych
- Pełnomocnika ds. Zintegrowanego Systemu Zarządzania – osoby odpowiedzialnej za doskonalenie Zintegrowanego Systemu Zarządzania

Za bezpieczeństwo informacji i ochronę danych osobowych odpowiedzialni są wszyscy pracownicy *Szpitala* oraz wszystkie osoby przetwarzające informacje w jego imieniu, niezależnie od formy współpracy. Wszystkie te osoby są zobowiązane do przestrzegania zasad bezpieczeństwa wynikających z niniejszej Polityki.

Wykorzystywanymi w organizacji kanałami komunikacji są:

- Strona internetowa,
- Intranet,
- Poczta elektroniczna, telefon, fax,
- Szkolenia,
- Przeglądy zarządzania,
- Spotkania, odprawy, dyskusje, narady,
- Materiały informacyjne i promocyjne (m.in. ulotki, broszury informacyjne, plakaty i tablice informacyjne, publikacje, informatory).

7. Podstawowe zasady bezpieczeństwa i ochrony danych osobowych

Zasady bezpieczeństwa powinny być przestrzegane przez wszystkich pracowników Szpitala, w celu zapewnienia bezpieczeństwa danych. Jest to niezmiernie ważne, ze względu na stopień wrażliwości danych, dotyczących przede wszystkim pacjentów oraz pracowników ochrony zdrowia.

Podstawowe zasady bezpieczeństwa, na których opiera się Polityka to:

- a) Zasada odpowiedzialności za czyny oraz zaniedbania dotyczące bezpieczeństwa informacji i ciągłości działania przez wszystkich pracowników w zakresie przetwarzanych przez nich informacji i realizowanych procesów,
- b) Zasada wiedzy koniecznej, polegająca na ograniczeniu dostępu do informacji wyłącznie w zakresie niezbędnym do wykonywania obowiązków,
- c) Zasada profesjonalizmu w wykonywaniu obowiązków, polegająca na przestrzeganiu ustalonych zasad oraz zaangażowaniu w zapewnienie bezpieczeństwa informacji i ochrony danych osobowych,
- d) Zasada poufności, polegająca na zapewnieniu, że informacje dotyczące funkcjonowania ZOZ w *Końskich* nie są udostępniane na zewnątrz osobom nieupoważnionym.
- e) Zasada bezzwłocznej reakcji na występujące incydenty zagrażające bezpieczeństwu informacji i ochrony danych osobowych oraz podejrzenia wystąpienia incydentu.

Pracownicy ZOZ w *Końskich* zobowiązują się do przestrzegania zasad Polityki Bezpieczeństwa informacji i Ochrony Danych Osobowych, podpisując stosowne oświadczenie.

8. Podnoszenie świadomości personelu

W celu zapewnienia poprawności funkcjonowania Polityki, Inspektor Ochrony Danych prowadzi szkolenia mające na celu ciągłe podnoszenie świadomości pracowników. Częstotliwość tych działań wynika z przeprowadzonej wcześniej analizy ryzyka oraz analizy zaistniałych incydentów bezpieczeństwa informacji.

9. Zarządzanie ryzykiem

W Zespole Opieki Zdrowotnej w *Końskich* opracowało i wdrożyło proces szacowania ryzyka zgodny z Rozporządzeniem Ogólnym w Zakresie Ochrony Danych Osobowych (RODO). Procesy te opisują kryteria dotyczące zasad oraz metod oceny ryzyka w systemie bezpieczeństwa informacji i ochrony danych osobowych.