POLITYKA BEZPIECZEŃSTWA INFORMACJI W PROJEKCIE

DEKLARACJA STOSOWANIA

Dyrektor Promotora Projektu, stojąc na stanowisku, że informacja jest priorytetowym zasobem Projektu, wdrożył System Zarządzania Bezpieczeństwem Informacji (SZBI). Bezpieczeństwo informacji oraz systemów, w których są one przetwarzane jest jednym z kluczowych elementów Podmiotów Leczniczych uczestniczących w Projekcie. Gwarancją sprawnej i skutecznej ochrony informacji jest zapewnienie odpowiedniego poziomu bezpieczeństwa oraz zastosowanie rozwiązań technicznych.

Dyrektor Promotora Projektu wprowadzając Politykę Bezpieczeństwa Informacji, deklaruje, że wdrożony System Zarządzania Bezpieczeństwem Informacji będzie podlegał ciągłemu doskonaleniu zgodnie z wymaganiami normy PN-ISO/IEC 27001 i 27799.

Podejście do bezpieczeństwa informacji w Projekcie opiera się na czterech kluczowych regułach:

- **Reguła poufności** - Zapewnienie stosowania zatwierdzonych ograniczeń w zakresie ujawniania i dostępu do informacji, w tym środków ochrony prywatności i informacji osobistych;
- **Reguła integralności** - Atrybut bezpieczeństwa informacji oznaczający, że informacja nie uległa nieuprawnionej modyfikacji lub zniszczeniu, w tym świadczący o niezaprzeczalności i autentyczności informacji.
- **Reguła dostępności** - Zapewnienie terminowego i niezawodnego dostępu do informacji i możliwość wykorzystania tej informacji;
- **Reguła rozliczalności** - Zdolność systemu, w którym działa podmiot do jednoznacznego określenia, jakie działania, kiedy i w odniesieniu do jakich obiektów ten podmiot wykonał.

Celem wdrożonego SZBI jest osiągnięcie poziomu organizacyjnego i technicznego, który:

- będzie gwarantem pełnej ochrony danych Pacjentów oraz ciągłości procesu ich przetwarzania,
- zapewni zachowanie poufności informacji chronionych, integralności i dostępności informacji chronionych oraz jawnych,

- zagwarantuje odpowiedni poziom bezpieczeństwa informacji, bez względu na jej postać, w systemach wykorzystywanych w Projekcie,
- maksymalnie ograniczy występowanie zagrożeń dla bezpieczeństwa informacji, które wynikają z celowej bądź przypadkowej działalności człowieka, sztucznej inteligencji lub botnetu oraz ich ewentualne wykorzystanie na szkodę Podmiotów Leczniczych uczestniczących w Projekcie,
- zapewni poprawne i bezpieczne funkcjonowanie wszystkich systemów przetwarzania informacji wykorzystywanych w Projekcie,
- zapewni gotowość do podjęcia działań w sytuacjach kryzysowych dla bezpieczeństwa Podmiotów Leczniczych, ich interesów oraz posiadanych i powierzonych im informacji.

Powyższe cele realizowane są poprzez:

- wyznaczenie osób odpowiedzialnych zapewniających optymalny podział i koordynację zadań związanych z zapewnieniem bezpieczeństwa informacji,
- wyznaczenie właścicieli dla kluczowych aktywów przetwarzających informację, którzy zobowiązani są do zapewnienia im możliwie jak najwyższego poziomu bezpieczeństwa,
- przyjęcie za obowiązujące przez wszystkich pracowników i współpracowników polityk i procedur bezpieczeństwa obowiązujących w Podmiotach Leczniczych,
- określenie zasad przetwarzania informacji, w tym stref w których może się ono odbywać,
- przegląd i aktualizację polityk i procedur postępowania dokonywaną przez odpowiedzialne osoby w celu jak najlepszej reakcji na zagrożenia i incydenty,

Dyrektor

Elżbieta Kasprzak