1. CEL

Określenie zasad bezpieczeństwa w zakresie dostępu do obszarów bezpiecznych Szpitala Rejonowego im. dr. Józefa Rostka w Raciborzu.

2. OPIS PROCESU

2.1. ODPOWIEDZIALNOŚĆ

1. **Dyrekcja Szpitala** odpowiada za zapewnienie środków na realizację inwestycji związanych z prawidłowym zabezpieczeniem i dostępem do budynku.
2. **Przewodniczący Zespołu ds. Zarządzania Bezpieczeństwem Informacji** jest odpowiedzialny za analizowanie sytuacji związanych z incydentami naruszenia zasad ochrony i zabezpieczenia dostępu do budynku.
3. **Pracownicy szpitala** odpowiadają za:
   - przestrzeganie zasad związanych z prawidłowym zabezpieczeniem i dostępem do budynku,
   - zgłaszanie przełożonemu wszelkich incydentów związanych z naruszeniem zasad bezpieczeństwa informacji.

2.2. TRYB POSTĘPOWANIA

1. Dostęp do pomieszczeń Szpitala mają wszystkie osoby zatrudnione i/ lub wykonujące prace na rzez Szpitala zgodnie zakresem obowiązków,
2. Pacjenci mogą sami przebywać tylko w salach szpitalnych i na korytarzach oczekując na przyjęcie.
3. Pracownicy opuszczający pomieszczenia i gabinety są zobowiązani zamykać drzwi na klucz. Zabrania się pozostawiania kluczy w drzwiach.
4. Pracownik który otrzymał klucze do pomieszczeń Szpitala zobowiązany jest chronić je przed zaginięciem,
5. Niedopuszczalne jest przekazywanie kluczy osobom spoza Szpitala.
6. Każdy pracownik po przyjściu do pracy zobowiązany jest potwierdzić swoją obecność odbijając na czytniku kartę magnetyczną, w przypadku jakichkolwiek dłuższych wyjść w godzinach pracy zawsze zobowiązany jest poinformować bezpośredniego przełożonego,
7. Niedopuszczalne jest pozostawianie pacjentów i osób nie mających nadanych uprawnień samych w pomieszczeniach, nawet w gabinecie lekarskim czy zabiegowym,
8. Niedopuszczalne jest umożliwienie dostępu osobom nieuprawnionym do dokumentów znajdujących się w pomieszczeniach szpitala. Osoby nieuprawnione po wejściu do pomieszczenia w którym przetwarzane są informacje, przyjmowane są przy wyznaczonych biurkach, stolikach lub ladach na których nie mogą znajdować się dokumenty oraz uruchomione stacje robocze.
9. Osoby trzecie wykonujące prace na rzecz Szpitala, których rodzaj prac związany jest z dostępem do zasobów informacyjnych zobowiązane są podpisać i złożyć w Rejestracji klauzulę poufności za wyjątkiem sytuacji gdzie klauzula o dochowaniu poufności informacji zawarta jest w umowie o współpracy.

10. Każdy pracownik jest zobowiązany do bezwzględnego stosowania zasad niniejszego dokumentu pod rygorem wyciągnięcia stosownych konsekwencji.

3. TERMINOLOGIA

Przyjęta z opracowaniu terminologia i skróty, zgodna jest z zasadami obowiązującymi w działającym Zintegrowanym Systemie Zarządzania oraz terminologią określoną w normach ISO 27000:2014, ISO 27001:2013, ISO 27002:2013.

- Zasoby Informacyjne lub Aktywa - wszystko, co posiada wartość dla organizacji z punktu widzenia bezpieczeństwa informacji,
- Dostępność - możliwość uzyskania i wykorzystania na żądanie przez uprawnioną jednostkę
- Poufność - cecha informacji, która nie jest udostępniana ani ujawniana nieupoważnionym osobom, jednostkom lub procesom
- Integralność - dokładność i kompletność zasobów
- Bezpieczeństwo informacji - ochrona poufności, integralności i dostępności informacji; mogą tu także należeć inne właściwości, takie jak autentyczność, odpowiedzialność, brak odrzucenia i niezawodność,
- Incydent związany z bezpieczeństwem informacji - pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, stwarzających znaczne prawdopodobieństwo zakłócenia lub zatrzymania działań biznesowych i zagrażających bezpieczeństwu informacji zwłaszcza w odniesieniu do poufności , integralności i dostępności.
- Zdarzenie związane z bezpieczeństwem informacji - zwane też zdarzeniem bezpieczeństwa – jest to określony stan systemu, usługi lub sieci, który wskazuje na niezgodność, błąd zabezpieczenia lub nieznana dotychczas sytuacja, która może być związana z bezpieczeństwem (może wpływać na bezpieczeństwo) i może być przyczyną incydentu lub słabością systemu
- Słabość systemu lub zabezpieczenia, aktywu – stan, sytuacja lub właściwość która, może spowodować wystąpienia incydentu lub zdarzenia związanego z bezpieczeństwem informacji.

4. DOKUMENTY ZWIĄZANE

Z niniejszą instrukcją związane są następujące dokumenty:

1. Zestaw norm dotyczących Bezpieczeństwa Informacji ISO 27000:2014, ISO 27001:2013, ISO 27002:2013.
2. Regulamin organizacyjny Szpital Rejonowy im. dr. Józefa Rostka w Raciborzu.
3. Dokumentacja ZSZJiŹS w wersji papierowej i elektronicznej.
4. Zarządzenia DN I DM dotyczące dokumentacji papierowej i elektronicznej

5. ZAŁĄCZNIKI

Brak

6. SPIS TREŚCI, KARTA ZMIAN, ZATWIERDZENIA.

1. Cel…… str 1
2. Opis procesu ……..str 1
3. Terminologia i skróty ……..str 2
4. Dokumenty związane ……str 2
5. Załączniki …… str 2
6. Spis treści, Karta zmian, Zatwierdzenia …….. str 3

Karta zmian

Nr zmiany	Zmiany		Opis zmiany	Data zmiany	Podpis autora zmiany
	Rozdz.	Strona			

Zatwierdzenia

Zespół	Imię i nazwisko KO	Data	Podpis
Opracował	Krzysztof Janicki	01.06.2017	*Podpis nieczytelny*
Sprawdził	Grzegorz Bula PZJ	01.06.2017	*Podpis nieczytelny*
Sprawdził	Maria Kroll NDG	01.06.2017	*Podpis nieczytelny*
Zatwierdził	Ryszard Rudnik	01.06.2017	*Podpis nieczytelny*