1. CEL

Celem procedury jest zapewnienie że:

1) proces szacowania ryzyka jest kompletny oraz daje szczegółowe, porównywalne i odtwarzalne rezultaty,
2) kryteria oceny ryzyka są ustanowione i spójne z rzeczywistym stanem bezpieczeństwa aktywów w Organizacji oraz dostarczają rzetelnych wyników na temat faktycznego poziomu ryzyka,
3) zidentyfikowano potencjalne ryzyko, opisano w kategoriach ilościowych i zarządza się nim świadomie,
4) dokumentacja szacowania ryzyka jest poddawana cyklicznym przeglądom oraz jest zatwierdzana przez kompetentny personel.

Celem procedury jest ustalenie metodyki oceny ryzyka bezpieczeństwa informacji oraz skutecznego pomiaru wyselekcjonowanych zabezpieczeń i grup zabezpieczeń poprzez mierniki oceny skuteczności. Na proces oceny ryzyka składa się:

a) przeprowadzenie szczegółowej oceny ryzyka w kontekście utraty integralności, poufności i/lub dostępności danego aktywa,
b) opracowanie planu postępowania z ryzykiem w oparciu o przyjęte kryteria akceptacji ryzyka z uwzględnieniem powtórnej analizy, w ramach wdrożonych działań zawartych w Planie postępowania z ryzykiem, zidentyfikowanych nowych podatności i zagrożeń oraz dokonanych incydentów dotyczących naruszenia bezpieczeństwa informacji.

Procedura swoim zakresem obejmuje wszystkie jednostki organizacyjne Organizacji po przeprowadzeniu inwentaryzacji aktywów zgodnie z procedurą *Analiza ryzyka bezpieczeństwa informacji*.

2.OPIS PROCESU

2.1 . ODPOWIEDZIALNOŚĆ

1) **Przewodniczący Zespołu ds. Zarządzania Bezpieczeństwem Informacji** jest odpowiedzialny za merytoryczne przygotowanie, rozpowszechnianie, analizowanie, zatwierdzanie oraz przechowywanie oryginałów dokumentów szacowania ryzyka.
2) **Kierownicy Komórek Organizacyjnych** są właścicielami określonych w dokumentach inwentaryzacyjnych aktywów, odpowiadają za bieżącą aktualizację oceny ryzyka bezpieczeństwa aktywów oraz przeprowadzanie okresowych przeglądów oceny ryzyka.
3) **Pracownicy szpitala** zobowiązani są zgłaszać zaobserwowane lub potencjalne zagrożenie oraz incydenty związane z bezpieczeństwem informacji, Kierownikowi KO któremu podlega.
4) „Właściciel ryzyka" – Kierownik KO prowadzący inwentaryzacje, jest odpowiedzialny za ryzyka związane z zinwentaryzowanymi aktywami w swojej komórce organizacyjnej.

2.2 . TRYB POSTĘPOWANIA

1. Ocena ryzyka

Istotą procesu oceny ryzyka jest określenie znaczenia ryzyka na podstawie porównania wyznaczonych wartości ryzyk dla zidentyfikowanych aktywów z kryteriami akceptowania ryzyka w kontekście celów strategicznych i biznesowych organizacji oraz spełnienia przepisów prawa. Ocena ryzyka powinna być prowadzona na

właściwym stopniu szczegółowości z uwzględnieniem strat finansowych, wizerunkowych i informacyjnych, które organizacja doświadczyła bądź może doświadczyć w przyszłości, polega to na przypisywaniu wartości liczbowej prawdopodobieństwu wystąpienia, podatności oraz skutkom zdarzeń.

Kierownik komórki organizacyjnej po przeprowadzeniu analizy ryzyka zgodnie z zasadami określonymi w procedurze *Inwentaryzacja i analiza ryzyka,* przedstawia opracowaną dokumentację (arkusze inwentaryzacyjne) do weryfikacji do Pełnomocnika ds. Bezpieczeństwa Informacji. Pełnomocnik po zweryfikowaniu dokumentów analizy ryzyka wspólnie z Zespołem ds. Bezpieczeństwa Informacji przeprowadza ocenę ryzyka na Arkuszu oceny ryzyka w programie Excel, osobno dla każdej grupy zinwentaryzowanych zasobów. W skład zespołu wchodzą wyznaczeni pracownicy.

2. Identyfikowanie potencjalnych zagrożeń i podatności

Ocena ryzyka przeprowadzana jest dla każdego zidentyfikowanego podczas inwentaryzacji aktywa, rozpatruje trzy obszary:

1) prawdopodobieństwo wystąpienia zagrożenia,
2) podatność aktywów na zagrożenia,
3) skutków potencjalnych zagrożeń,

biorąc pod uwagę następstwa naruszenia lub utraty:

5) poufności,
6) integralności,
7) dostępności,

które mogą nastąpić w wyniku działań:

8) umyślnych - (U),
9) przypadkowych – (P),
10) naturalnych - (N).

Przyjmuje się, że zagrożenia (U,P) są wynikiem działań ludzkich, natomiast źródła zagrożeń (N) są niezależne od człowieka.

Przykładową listę potencjalnych i realnych dla Organizacji zagrożeń umieszczono w Tabeli nr 1. Wymienione zagrożenia należy uwzględnić podczas szacowania prawdopodobieństwa, podatności oraz skutków zdarzeń. W przypadku wystąpienia ryzyka nieakceptowanego należy w „Arkuszach oceny ryzyka", wpisać nazwę zagrożenia, wybranego z Tabeli nr 1, w kolumnie „Potencjalne Zagrożenie".

Należy uwzględnić, że podatność, nie powoduje jeszcze szkody, ale należy zgodnie Tabeli nr 2 oszacować stopień zabezpieczenia aktywa pod kątem zidentyfikowanych zagrożeń.

Tabela nr1 Typowe zagrożenia – przykłady

Numer zagrożenia	Rodzaj	Zagrożenie	Źródło
1	Zniszczenia fizyczne	pożar, zalanie , zanieczyszczenie, poważny wypadek, zniszczenie urządzeń lub nośników, pył, korozja, wychłodzenie	P, U, N

2	Zjawiska naturalne	zjawiska klimatyczne, zjawiska pogodowe, powódź	N
3	Naruszenie bezpieczeństwa informacji	podsłuch, kradzież nośników lub dokumentów, kradzież urządzenia, szpiegostwo, kopiowanie danych, odtworzenie wyrzuconych nośników	U
		ujawnienie informacji, dane z niewiarygodnych źródeł, sfałszowanie oprogramowania,	P, U
4	Awarie techniczne	awaria urządzenia, niewłaściwe funkcjonowanie urządzenia, niewłaściwe funkcjonowanie oprogramowania	P
		umyślne uszkodzenie urządzenia lub oprogramowania	U
5	Utrata usług	awaria systemu klimatyzacji, utrata dostaw prądu, awaria urządzenia telekomunikacyjnego	P, U, N
6	Zakłócenia spowodowane promieniowaniem	promieniowanie elektromagnetyczne, promieniowanie cieplne, impuls elektromagnetyczny	P, U, N
7	Nieautoryzowanie działania	niewłaściwe funkcjonowanie urządzeń, niewłaściwe funkcjonowanie oprogramowania	P
		przeciążenie systemu informacyjnego, naruszenie zdolności utrzymania systemu informacyjnego	P, U
8	Naruszenie bezpieczeństwa funkcji	błąd użytkowania	P
		naruszenie praw	P, U
		fałszowanie praw, odmowa działania	U
		naruszenie dostępności personelu	P, U, N

Tabela nr 2 Typowe podatności - przykłady

Rodzaj	Przykład podatności	Przykłady zagrożeń
Sprzęt	Niezabezpieczone urządzenie do przechowywania danych	Kradzież danych lub dokumentów
	Brak staranności przy pozbywaniu się nośników	Kradzież nośników lub danych
	Niekontrolowane kopiowanie	Kradzież danych
	Wrażliwość na wilgoć, pył, zanieczyszczenie	Pył, korozja, wychłodzenie
	Wrażliwość na zmiany temperatury	Zjawiska pogodowe lub aspekty produkcyjne
	Wrażliwość na zmiany napięcia zasilania	Utrata zasilania

	Brak planów okresowej wymiany sprzętu	Zniszczenie lub awaria urządzenia lub nośników
Oprogramowanie	Brak wylogowania przy opuszczaniu stacji roboczej	Nadużycie praw
	Błędne przypisanie praw dostępu	Nadużycie praw
	Brak mechanizmów identyfikacji i uwierzytelnienia użytkownika	Fałszowanie praw
	Złe zarządzanie hasłami	Fałszowanie praw
	Brak fizycznej kontroli budynków, drzwi i okien	Kradzież nośników lub danych
	Brak skutecznej kontroli zmian	Zakłócenie procesu
Sieć	Niezabezpieczone linie telefoniczne	Podsłuch
	Złe łączenie kabli	Awaria urządzenia telekomunikacyjnego
	Brak identyfikacji i uwierzytelniania nadawcy i odbiorcy	Fałszowanie praw
	Niezabezpieczone połączenie z siecią publiczną	Nieautoryzowane użycie urządzeń
	Uszkodzenie fizyczne sieci lub kabli	Zatrzymanie procesu
Personel	Nieobecność personelu	Naruszenie danych
	Niewystarczające szkolenie z bezpieczeństwa, użycia oprogramowania lub sprzętu	Błąd użytkowania
	Brak mechanizmów monitorowania	Nielegalnie przetwarzanie danych
	Praca personelu zewnętrznego lub sprzątającego bez nadzoru	Nieautoryzowane użycie urządzeń
Siedziba	Lokalizacja na obszarach zagrożonych powodzią	Powódź
	Brak fizycznej ochrony budynków, drzwi i okien	Kradzież, zniszczenie
Organizacja	Brak procedur regulujących bezpieczeństwo aktywów	Utrata danych
	Brak regularnego nadzoru	Nadużycie praw
	Brak zdefiniowanego postępowania dyscyplinarnego	Kradzież urządzenia

3. Metodyka Oceny Ryzyka

Metodyka Oceny Ryzyka w Organizacji, została ustanowiona w zgodzie z rzeczywistym stanem bezpieczeństwa aktywów w organizacji, oraz dostarcza rzetelnych wyników na temat faktycznego poziomu ryzyka. Ocena ryzyka przeprowadzana jest w *Arkuszu Oceny Ryzyka* w programie EXCEL. dane wejściowe do procesu oceny uważa się wszelkie informacje przedstawione w analizie ryzyka (dane z inwentaryzacji), a w szczególności miejsce, obecne zabezpieczenia oraz wagę przypisaną przez właściciela aktywa. Ponadto każde szacowanie prawdopodobieństwa, podatności oraz skutków zdarzenia powinno się odbywać w relacji z Tabelą nr 1 i 2 niniejszej procedury według zadanych kryteriów. Określając skutek należy wziąć pod uwagę wagę aktywu określoną w tabeli inwentaryzacyjnej. Podczas oceny ryzyka należy uzupełnić kolumnę „Właściciel ryzyka" w dokumencie oceny ryzyka w programie EXCEL. Za aktualność oceny ryzyka odpowiedzialny jest „Właściciel ryzyka".

Szacowanie prawdopodobieństwa Tabela nr.3

Badane kryterium	Ryzyko	Wartość
(PO) Prawdopodobieństwo *(możliwość wystąpienia)*	niskie, odległe, mało realne szanse na zdarzenie	1
	może się zdarzyć lub zdarza się sporadycznie	2
	bardzo realne szanse wystąpienia	3

Szacowanie podatności Tabela nr.4

Badane kryterium	Ryzyko	Wartość
(PR) Podatność *(słabość aktywa)*	aktywa bardzo dobrze zabezpieczone	1
	aktywa dostatecznie zabezpieczone	2
	aktywa słabo lub nie zabezpieczone	3

Szacowanie skutków Tabela nr.5

Badane kryterium	Ryzyko	Wartość
(S) Skutek *(wpływ na organizację i/lub proces)*	utrata danych nie spowoduje utrudnień w pracy przedsiębiorstwa lub danego procesu, odtworzenie danych nie wymaga dużych nakładów czasu	1
	utrata danych spowoduje zakłócenia w funkcjonowaniu i/lub wizerunku przedsiębiorstwa , odtworzenie danych jest możliwe ale pracochłonne	2
	utrata danych spowoduje zatrzymanie procesu i/lub wywoła poważne konsekwencje prawne, odtworzenie danych i reputacji będzie trudne i kosztowne.	3

4. Kategoria Ryzyka

Kategoria ryzyka zostaje ustanowiona zgodnie ze wzorem:

R = PR · PO · S

gdzie:

PR - Prawdopodobieństwo

PO - Podatność

S - Skutek

Wynik z działania zgodnie z poniższą tabelą należy przypisać ustanowionym kategoriom ryzyka, a następnie uruchomić czynności doskonalące bezpieczeństwo informacji w celu redukcji ryzyka do poziomu akceptowalnego w ramach Planu postępowania z ryzykiem. W uzasadnionych przypadkach Pełnomocnik w konsultacji z Najwyższym Kierownictwem może zaakceptować ryzyko kategorii drugiej lub trzeciej, szczególnie gdy działania profilaktyczne odnoszą się do długoterminowych i kosztownych inwestycji na rzecz bezpieczeństwa danego aktywa.

Wytyczne do postępowania z ryzykiem Tabela nr.6

Klasa Kategorii	Kategoria Ryzyka	Wartość Ryzyka	Akceptacja Ryzyka Tak / Nie	Działania zapobiegawcze
1	Małe	1÷ 8	**TAK**	Podejmowanie działań nie jest konieczne, zalecane jest utrzymywanie ryzyka na obecnym poziomie. Można podjąć działania doskonalące
2	Średnie	9 ÷ 17	**NIE**	Należy zredukować ryzyko do poziomu akceptowalnego poprzez rozwiązania infrastrukturalne i/lub proceduralne
3	Duże	**18 ÷ 27**	**NIE**	Należy zdecydowanie zredukować ryzyko do poziomu akceptowalnego poprzez rozwiązania infrastrukturalne i/lub proceduralne usuwając lub przenosząc aktywa w bezpieczniejsze miejsce.

5. Działania doskonalące bezpieczeństwo informacji

Procesy doskonalące bezpieczeństwo informacji prowadzone są w oparciu o podjęte działania zapobiegawcze i/lub korygujące adekwatnie do wagi potencjalnych problemów. W tym celu Pełnomocnik uruchamia plan postępowania z ryzykiem. Wyniki działań przeprowadzonych na podstawie założeń zawartych w planie postępowania z ryzykiem, należy według powyższych zasad powtórnie poddać ocenie ryzyka w celu sprawdzenia skuteczności i odporności systemu na przypadek zaistnienia zadanych w pierwszej fazie oceny

zagrożeń naruszających poufność, dostępność i/lub integralność. Wynik z powtórnej analizy stanowi o ryzyku szczątkowym, które jest pozostałością po podjęciu wszystkich możliwych kroków zmierzających do unikania ryzyka, jego kontrolowania lub przeniesienia (transferu)

6. Plan postępowania z ryzykiem

Pełnomocnik dla aktywów gdzie ryzyko buło nieakceptowalne, formułuje plan postępowania z ryzykiem, w którym określone zostają odpowiednie działania, odpowiedzialności oraz chronologiczne priorytety w celu redukcji ryzyka do poziomu bezpiecznego – akceptowalnego. W tym celu Pełnomocnik w porozumieniu z kierownictwem komórki, której działania dotyczą wdraża adekwatne do wynikającego ryzyka zabezpieczenia oraz mierzy ich skuteczność. Pomiar skuteczności odbywa się w relacji z Załącznikiem A Normy PN-ISO/IEC 27001:20013 *(Cele stosowania zabezpieczeń i zabezpieczenia)* – Zabezpieczenie uważa się za skuteczne, gdy posiada wszelkie cechy narzucone przez Normę.

Ostatecznie zatwierdzone i wdrożone zabezpieczenia należy wpisać w Dokument oceny ryzyka w kolumnie działań zapobiegawczych i/lub korygujących w celu poddania aktywa ponownej ocenie ryzyka.

7. Wprowadzanie zmian

Dokonywanie zmian w ocenie ryzyka odbywa się w wyniku każdorazowego podjęcia działań korygujących i/lub zapobiegawczych, zidentyfikowania nowego - realnego zagrożenia oraz dokonanego incydentu naruszającego bezpieczeństwo informacji.

Zapisy sporządzone w ocenie ryzyka nie ulegają przedawnieniu i są trwałe, w związku z czym każde działanie mające na celu ponowną ocenę ryzyka bezwzględnie dokonuje się w kolejnym cyklu analizy.

3. TERMINOLOGIA I SKRÓTY

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.
- Podatność – słabość aktywu lub grupy aktywów, która może być wykorzystana przez co najmniej jedno zagrożenie.
- Stacja robocza – komputer wraz z monitorem, klawiaturą, głośnikami i myszką

Szpital – Szpital Rejonowy im. dr. Józefa Rostka w Raciborzu

PZJ - Pełnomocnik ds. Zarządzania Jakością.

ZSZ – Zintegrowany System Zarządzania Jakością i Bezpieczeństwem informacji.

KO – Komórka organizacyjna Szpitala.

KKO - Kierownik KO

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 ZSZJiZŚ w wersji papierowej i elektronicznej.
4. Zarządzenia DN I DM dotyczące dokumentacji papierowej i elektronicznej
5. Procedura - Inwentaryzacja i analiza ryzyka

5. ZAŁĄCZNIKI

1. FZSZ-7.1- Arkusz oceny ryzyka nr 1- **Aktywa informacyjne** (dokument elektroniczny)
2. FZSZ-7.2- Arkusz oceny ryzyka nr 2- **Aktywa fizyczne** (dokument elektroniczny)
3. FZSZ-7.3- Arkusz oceny ryzyka nr 3- **Infrastruktura pomocnicza** (dokument elektroniczny)
4. FZSZ-7.4- Arkusz oceny ryzyka nr 4- **Pracownicy** (dokument elektroniczny)

6. SPIS TREŚCI, KARTA ZMIAN, ZATWIERDZENIA.

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	01.06.2017	*Podpis nieczytelny*
Zatwierdził	Ryszard Rudnik	01.06.2017	*Podpis nieczytelny*