2. Deklaracja Polityki Bezpieczeństwa Informacji

Dyrektor Szpitala rozumiejąc, że informacja jest jednym z najważniejszych aktywów każdej organizacji, wdrożył system zarządzania bezpieczeństwem informacji, którego głównym celem jest zapewnienie poufności, integralności, dostępności informacji oraz zabezpieczenie przed nieautoryzowanym dostępem lub zniszczeniem zasobów, które biorą udział w przechowywaniu, przesyłaniu oraz przetwarzaniu informacji. Środki podjęte do ochrony zasobów oraz zakres ochrony są odpowiednie do zakresu przetwarzanych informacji oraz uwzględniają cele biznesowe Szpitala.

Szpital zapewnia bezpieczeństwo informacji poprzez:

- ✓ zarządzanie ryzykiem, w ramach którego przeprowadza się ocenę wartości zasobów i klasyfikację informacji, identyfikację poziomów zagrożeń i ich konsekwencji; pod uwagę bierze się takie kryteria jak ryzyko, skutki oraz miejsce utraty informacji; podejmuje się również działania mające na celu zdefiniowanie sposobów zarządzania zabezpieczeniami zasobów,
- ✓ zarządzanie zmianami, w ramach którego prowadzi się analizę zmian pod względem ich wpływu na poziom bezpieczeństwa oraz zapewnienie pełnej koordynacji podczas wprowadzania zmian,
- ✓ zarządzanie ciągłością działania Szpitala przez określenie, wdrożenie i utrzymanie Planu postępowania na wypadek sytuacji nadzwyczajnej na terenie Szpitala.

Główne cele systemu zarządzania bezpieczeństwem informacji to:

- ✓ zapewnienie dostępności do informacji osobom upoważnionym,
- ✓ zabezpieczenie informacji, dokumentów, systemów przetwarzających informacje przed nieautoryzowanym dostępem, modyfikacją lub zniszczeniem,
- ✓ minimalizowanie ryzyka utraty informacji,
- ✓ zaangażowanie wszystkich pracowników w ochronę informacji,
- ✓ zwiększanie świadomości pracowników,
- ✓ monitorowanie korzystania z danych osobowych oraz medycznych na wszystkich etapach ich przetwarzania przed nieautoryzowanym dostępem, zmianą, kopiowaniem, zniszczeniem,
- ✓ zapewnienie zgodności z prawem obowiązującym na terytorium RP w zakresie ochrony danych osobowych oraz zgodności z umowami.

Dyrekcja Szpitala podejmuje działania związane z zapewnieniem środków niezbędnych do realizacji Polityki Bezpieczeństwa Informacji (ogólnej i szczegółowej). W Szpitalu został powołany Komitet ds. Bezpieczeństwa, którego głównymi zadaniami są: wyznaczanie i aktualizacja celów stosowania zabezpieczeń, technik zabezpieczeń oraz zarządzanie klasyfikacją informacji i szacowaniem ryzyka. W skład Komitetu wchodzą pracownicy z komórek organizacyjnych Szpitala mające istotny wpływ na poziom bezpieczeństwa informacji w Szpitalu.

Role, uprawnienia i odpowiedzialności osób odpowiedzialnych za zarządzaniem bezpieczeństwem informacji zostały określone w Załączniku nr 5 do niniejszego dokumentu oraz pozostałej dokumentacji bezpieczeństwa informacji. Pracownicy Szpitala oraz podmioty zewnętrzne są zobowiązani do zapoznania się i respektowania postanowień dokumentacji bezpieczeństwa informacji.

Dla realizacji celów opisanych w deklaracji stosowania mających za zadanie zapewnienie skutecznego funkcjonowania systemu zarządzania bezpieczeństwem informacji zgodnego z wymaganiami normy PN-ISO/IEC 27001:2007 ustanowione zostały zabezpieczenia. Zbiór zabezpieczeń, powodów stosowania tych zabezpieczeń jak i cele wybranych do stosowania w Szpitalu zabezpieczeń zostały zebrane oraz wymienione w „Deklaracji stosowania" stanowiącej Załącznik nr 6 do niniejszego dokumentu. Za nadzorowanie jej zmian, aktualizację oraz nadzór nad realizacją wymogów okresowego monitorowania odpowiedzialny jest Pełnomocnik ds. Bezpieczeństwa.

2.1 System zabezpieczeń danych osobowych (środki techniczne i organizacyjne)

Każdy ma prawo do ochrony dotyczących go danych osobowych. Prawo to reguluje ustawa o ochronie danych osobowych oraz rozporządzenie MSWiA w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Instrukcja zarządzania systemem informatycznym przetwarzającym dane osobowe zawiera:

- ✓ wykaz budynków tworzących obszar, w którym przetwarzane są dane osobowe,
- ✓ wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
- ✓ opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi określenie sposobu przepływu danych pomiędzy poszczególnymi systemami.

Dostęp do danych osobowych mogą mieć tylko osoby posiadające pisemne, imienne upoważnienia. Osoby upoważnione mają dostęp do danych osobowych zgodnie z zasadą przywilejów koniecznych, tylko w takim zakresie w jakim jest im to niezbędne do wykonywania obowiązków służbowych.

Dane osobowe, powinny być zabezpieczone zgodnie z ustanowionymi zasadami bezpieczeństwa, a każdy z użytkowników powinien zachować szczególną ostrożność przy przetwarzaniu wszelkich danych osobowych

stosując się do zasad określonych w Regulaminie użytkownika systemu informatycznego - Załącznik nr 7 do niniejszego dokumentu.

Zbiór zasad ustalonych w dokumentacji SZBI ma zastosowanie do wszystkich zbiorów danych osobowych administrowanych przez Szpital w szczególności do:

- ✓ wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych, w których przetwarzane są lub będą dane osobowe podlegające ochronie,
- ✓ danych osobowych (wrażliwych) przetwarzanych w dowolnej formie (np. elektronicznej, papierowej),
- ✓ danych osobowych zarówno w przypadku, gdy Szpital jest administratorem danych, jak i w sytuacji, gdy przetwarza dane powierzone mu na podstawie umów zawartych w trybie art. 31 ustawy o ochronie danych osobowych,
- ✓ wszystkich nośników informacji, np. papierowych, magnetycznych, optycznych itp., na których są lub będą znajdować się dane osobowe podlegające ochronie,
- ✓ wszystkich pomieszczeń, w których są lub będą przetwarzane dane osobowe podlegające ochronie,
- ✓ wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, stażystów, praktykantów i innych osób (strony trzecie) mających dostęp do danych osobowych podlegających ochronie.

Szczegółowe zasady wydawania upoważnień, nadawania, zmiany i cofania uprawnień określone są w Procedurze PR-04 QBP-02 System kontroli dostępu.

W przypadku naruszenia zasad dotyczących bezpieczeństwa przetwarzanych informacji zawierających dane osobowe należy postępować zgodnie z Instrukcją Postępowania w sytuacji naruszenia ochrony danych osobowych zawartą w Rozdziale 8 niniejszego dokumentu.

3. Organizacja bezpieczeństwa informacji

Kluczowe z punktu widzenia funkcjonowania systemu zarządzania bezpieczeństwem informacji jest odpowiednie ustalenie odpowiedzialności i obowiązków stron odpowiedzialnych za funkcjonowanie systemu. Niniejsza Polityka określa podstawowe obowiązki pracowników odpowiedzialnych za bezpieczeństwo informacji i zasobów.

3.1 Role w ramach struktury organizacyjnej

Zarządzanie bezpieczeństwem informacji w Szpitalu odbywa się w oparciu o ustanowione poniżej role (funkcje). Obowiązkiem Szpitala jest wskazanie konkretnego pracownika (stanowisko), odpowiedzialnego ze realizację działań dla ustanowionych ról. Dla każdej ustanowionej roli przypisano obszar działań dotyczących bezpieczeństwa informacji. Wykaz osób pełniących kluczową rolę w ramach SZJiZBI zamieszczono w Załączniku nr 3 do niniejszego dokumentu.

3.1.1 Dyrektor Szpitala

Dyrektor Szpitala odpowiedzialny jest za zaangażowanie w proces utrzymania systemu zarządzania bezpieczeństwem informacji oraz podejmowanie działań w celu zapewnienia zasobów niezbędnych do funkcjonowania tego systemu. W szczególności do obowiązków Dyrektora należy:

- ✓ zatwierdzenie Polityki Bezpieczeństwa Informacji wraz z dokumentami towarzyszącymi (regulaminy, procedury, instrukcje, plany, deklaracja stosowania),
- ✓ zatwierdzenie zmian Polityki Bezpieczeństwa Informacji wraz z dokumentami towarzyszącymi,
- ✓ ustanowienie struktury zarządzania bezpieczeństwem informacji – powołanie Komitetu ds. Bezpieczeństwa,
- ✓ powołanie Pełnomocnika ds. Bezpieczeństwa oraz administratorów poszczególnych obszarów bezpieczeństwa,
- ✓ zatwierdzanie wyników analizy ryzyka i planów postępowania z ryzykiem,
- ✓ podejmowanie działań w celu zapewnienia dostępności zasobów niezbędnych do utrzymania funkcjonowania systemu zarządzania bezpieczeństwem informacji,
- ✓ zapewnienie finansowania przedsięwzięć z zakresu bezpieczeństwa informacji,
- ✓ podejmowanie strategicznych decyzji w zakresie bezpieczeństwa informacji.

3.1.2 Komitet ds. Bezpieczeństwa

Komitet ds. Bezpieczeństwa odpowiedzialny jest za koordynowanie działań związanych z bezpieczeństwem informacji przez reprezentantów różnych obszarów Szpitala pełniących odpowiednie role. Obowiązki oraz uprawnienia członków Komitetu ds. Bezpieczeństwa zostały określone w Załączniku nr 5 do niniejszego dokumentu.

3.1.3 Autor publikacji

Autorem publikacji jest każda osoba, która powoduje utrwalenie informacji w formie papierowej, elektronicznej lub innej. Autor każdej publikacji odpowiedzialny jest za:

- ✓ określenie klasy dokumentu zgodnie z przyjętą klasyfikacją informacji,
- ✓ oznaczenie dokumentu zgodnie z wymaganiami Polityki Bezpieczeństwa Informacji i wymaganiami klasyfikacji informacji.

Minimalne wymagania dotyczące kompetencji: szkolenie w zakresie systemu zarządzania bezpieczeństwem informacji.

3.1.4 Redaktor publikacji

Redaktorem publikacji jest każdy pracownik Szpitala, który zleca lub nadzoruje utrwalenie informacji. Redaktor każdej publikacji odpowiedzialny jest za:

- ✓ weryfikację informacji przeznaczonych do publikacji pod kątem zgodności z przyjętą klasyfikacją informacji,
- ✓ zatwierdzanie informacji do publikacji w środkach publicznie dostępnych,
- ✓ okresową weryfikację publikacji i jej aktualności w środkach publicznie dostępnych (w celu ograniczenia nieautoryzowanej treści publikacji).

Minimalne wymagania dotyczące kompetencji: szkolenie w zakresie systemu zarządzania bezpieczeństwem informacji.

3.1.5 Kierownicy komórek organizacyjnych w Szpitalu

Kierownicy poszczególnych komórek organizacyjnych w Szpitalu w ramach udziału w procesie zarządzania bezpieczeństwem informacji odpowiedzialni są za:

- ✓ wdrażanie Polityki Bezpieczeństwa Informacji i planów postępowania z ryzykiem w ramach kompetencji w podległych im komórkach organizacyjnych,
- ✓ podejmowanie działań w celu zapewnienia zasobów niezbędnych do utrzymania funkcjonowania systemu zarządzania bezpieczeństwem informacji,
- ✓ podejmowania działań w celu określenia zasad właściwego korzystania z zasobów i informacji w ramach podległej komórki organizacyjnej,
- ✓ nadzór nad bezpieczeństwem informacji w ramach kompetencji w podległych im komórkach organizacyjnych,
- ✓ uczestnictwo w analizie ryzyka bezpieczeństwa informacji w zakresie podległych im komórek i wdrażanie działań wynikających z przeprowadzonej analizy.

3.1.6 Pracownik (użytkownik)

Każdy pracownik odpowiedzialny jest za:

- ✓ stosowanie procedur wynikających z dokumentacji SZBI,
- ✓ jakość świadczonych usług dla klientów oraz tworzenie bezpiecznego środowiska pracy,
- ✓ wypełnianie swoich obowiązków określonych w dokumentacji przechowywanej w aktach osobowych,
- ✓ stosowanie i przestrzeganie przyjętych zasad i postanowień określonych w dokumentacji SZBI,
- ✓ przestrzeganie zasad ochrony danych osobowych określonych w Polityce Bezpieczeństwa Informacji i dokumentach z nią związanych,
- ✓ przetwarzanie danych osobowych zgodnie z celami ich przetwarzania,
- ✓ zapewnienie bezpieczeństwa danych osobowych, do których uzyskują dostęp w ramach pełnienia obowiązków służbowych,
- ✓ zachowanie szczególnej staranności w trakcie wykonywania operacji przetwarzania danych osobowych w celu ochrony interesów osób, których te dane dotyczą,
- ✓ informowanie Administratora Bezpieczeństwa lub Pełnomocnika ds. Bezpieczeństwa o wszelkich zauważonych nieprawidłowościach skutkujących obniżeniem poziomu bezpieczeństwa (poufność, integralność, dostępność) danych osobowych,
- ✓ współpracę z Komitetem Bezpieczeństwa w zakresie bezpieczeństwa informacji.

3.2 Upoważnienia i zgody

Przez zgodę rozumiane jest wyrażenie aprobaty przełożonego lub wskazanej w dokumentacji bezpieczeństwa informacji osoby na wykonanie konkretnej czynności przez określoną osobę.

Przez czasowe upoważnienie rozumiane jest wyrażenie aprobaty przełożonego lub wskazanej w dokumentacji bezpieczeństwa informacji osoby na wykonywanie określonego rodzaju czynności przez określoną osobę w oznaczonym okresie czasu.

Przez stałe upoważnienie rozumiane jest wyrażenie aprobaty przełożonego lub wskazanej w dokumentacji bezpieczeństwa informacji osoby na wykonywanie określonego rodzaju czynności przez określoną osobę aż do odwołania upoważnienia.

Pod nieobecność przełożonego lub wskazanej w dokumentacji bezpieczeństwa informacji osoby upoważnienie lub zgodę może wydać osoba upoważniona do zastępstwa.

Wszędzie tam, gdzie w niniejszej Polityce mowa jest o udzielaniu zgody (upoważnienia) w formie pisemnej należy przez to rozumieć pismo podpisane odręcznie, wiadomość poczty elektronicznej lub wpis do systemu informatycznego mającego funkcjonalność zapisywania i prezentowania osoby (lub konta informatycznego o uwierzytelnionym dostępie), która dokonała wpisu.

3.3 Porozumienia i kontakty ze stronami zewnętrznymi

Współpraca Szpitala z podmiotem zewnętrznym może mieć wpływ na funkcjonowanie kluczowych elementów systemu zarządzania bezpieczeństwem informacji. Współpraca ta realizowana jest w oparciu o zawartą z tym podmiotem umowę. Szczegółowe zasady dotyczące tworzenia umów reguluje Zarządzenie Dyrektora Nr 39/2010 w sprawie wprowadzenia Instrukcji dotyczącej "Zasad tworzenia, obiegu i rejestracji umów zawieranych przez Wojewódzki Szpital Specjalistyczny im. M. Kopernika w Łodzi. Do zawierania umów z podmiotami zewnętrznymi upoważniony jest jedynie Dyrektor Szpitala a pod jego nieobecność upoważniony Zastępca.

Ogólne zasady dotyczące współpracy z dostawcami zostały określone w procedurze systemowej PR-07 QBP-01 Realizacja dostaw.

W kontaktach z podmiotami zewnętrznymi Szpital reprezentowany jest przez Dyrektora lub osobę upoważnioną do realizacji określonego zadania.

3.4 Procedury systemu zarządzania bezpieczeństwem informacji

Dokumentacja bezpieczeństwa informacji jest nadzorowana przez Pełnomocnika ds. Bezpieczeństwa i jest dostępna dla wszystkich zainteresowanych osób (pracowników Szpitala) z wyjątkiem dokumentów o charakterze poufnym. Aktualne dokumenty są umieszczone w intranecie Szpitala.

Zasady określone w Polityce Bezpieczeństwa Informacji są realizowane są w Szpitalu zgodnie z procedurami systemowymi określonymi w Księdze Jakości Zintegrowanego Systemu Zarządzania Jakością i Zarządzania Bezpieczeństwem Informacji.

3.4.1 Nadzór nad dokumentami i zapisami

Wszystkie dokumenty systemu zarządzania bezpieczeństwem informacji powinny być aktualne, zatwierdzone i dostępne dla uprawnionych pracowników. Wszystkie egzemplarze dokumentacji w postaci papierowej należy traktować jako nadzorowane. Egzemplarze w postaci elektronicznej należy traktować jako nienadzorowane, chyba, że w jawny sposób są oznaczone jako nadzorowane.

W każdym obszarze działalności wyszczególnione zostały zapisy (dowody wykonania określonych działań), wskazane zostały osoby odpowiedzialne za nadzór nad zapisami. Kierownicy poszczególnych komórek organizacyjnych w Szpitalu pełnią nadzór kierowniczy nad zapisami – kontrolują, by zapisy wykonywano w sposób właściwy.

Dokumentacja bezpieczeństwa informacji jest opracowana zgodnie wymogami szczegółowej procedury nadzoru nad dokumentami i zapisami. Dla zapewnienia jednolitego sposobu tworzenia, ewidencjonowania i przechowywania dokumentów należy zapewnić zgodność Instrukcji Kancelaryjnej z wymaganiami szczegółowymi procedur.

Wszystkie dokumenty zawierające dane osobowe (w tym dane medyczne) podlegają ochronie zgodnie z zasadami określonymi w Załączniku nr 4 – Klasyfikacja informacji. Zasady te dotyczą zarówno oryginałów jak również każdej kopii, niezależnie od rodzaju nośnika na jakim zostały utrwalone.

3.4.2 Działania zapobiegawcze, korekcyjne oraz korygujące, postępowanie z incydentem

Skuteczne funkcjonowanie systemu zarządzania bezpieczeństwem informacji powinno opierać się na wiedzy odnośnie występowania podatności, zagrożeń, zdarzeń oraz incydentów bezpieczeństwa. Dlatego też niezbędne jest zgłaszanie informacji o zagrożeniach, zdarzeniach oraz incydentach. Uzyskiwane informacje służą do podejmowania działań naprawczych i doskonalących (korygujących lub zapobiegawczych). Ich celem jest zapewnienie szybkiej, efektywnej i uporządkowanej reakcji na zdarzenia związane z bezpieczeństwem informacji, w tym wyjaśnienie przyczyn, przypisania odpowiedzialności i określenia wniosków co do zakresu działań zapobiegawczych w przyszłości. Obowiązujące w tym zakresie zasady zostały spisane w Procedurze PR-03 QBP-002/S Nadzór nad niezgodnościami. Działania zapobiegawcze, korekcyjne oraz korygujące.

3.4.3 Audity wewnętrzne

Audity wewnętrzne służą weryfikacji czy ustanowiony Zintegrowany System Zarządzania jest zgodny z wymaganiami określonych norm i standardów, czy działania przebiegają zgodnie z opracowaną dokumentacją systemu zarządzania oraz czy system ten jest skutecznie wdrożony i utrzymywany. Audyty wewnętrzne są planowane i przeprowadzane zgodnie z Procedurą systemową PR-03 QBP-003/S Audit wewnętrzny.

3.4.4 Kompetencje, podnoszenie świadomości oraz szkolenia

Wszyscy pracownicy Szpitala wykonujący swoje zadania mają wpływ na jakość świadczonych usług oraz bezpieczeństwo przetwarzanych informacji. Dlatego wszyscy pracownicy powinni posiadać odpowiednie kompetencje do wykonywania zadań oparte na odpowiednim wykształceniu, szkoleniach, umiejętnościach i doświadczeniu. Wymagania te zostały określone w Procedurze PR-04 QBP-01. Dla zapewnienia ciągłego doskonalenia i osiągania optymalnych efektów w działalności Szpitala, prowadzone są okresowe szkolenia zgodnie z w/w procedurą.

3.4.5 Nadzorowanie zakupów

Proces zakupów powinien być zgodny z przepisami prawnymi regulowanymi przez prawo zamówień publicznych. Procedura dokonywania zakupów w Szpitalu odbywa się na podstawie opracowanego Regulaminu Zamówień Publicznych.

Podczas realizacji umów zakupionych towarów i usług odbywa się weryfikacja dostarczonego wyrobu lub usługi pod kątem jej zgodności z wymaganiami specyfikacji istotnych warunków zamówienia (SIWZ) oraz zgodności z warunkami umowy. Proces ten odbywa się zgodnie z Procedurą systemową PR-07 QBP-01 Realizacja dostaw.

3.4.6 Przeglądy kierownictwa

Ustanowiony Zintegrowany System Zarządzania wymaga, aby kierownictwo Szpitala dokonywało regularnych przeglądów systemu. Głównym celem realizacji przeglądu jest zapoznanie kierownictwa z aktualnym stanem systemu zarządzania oraz podjęcie decyzji związanych z jego dalszym funkcjonowaniem. Tematyka ta została szczegółowo opisana w Księdze ZSZJiBI.

3.4.7 Aktywa

Pracownikom powierza się aktywa Szpitala w celu realizacji zleconych im zadań. Aktywa są tym wszystkim, co stanowi wartość dla Szpitala np. narzędzia, urządzenia, materiały, wyposażenie itp. Za znajdujące się w komórce organizacyjnej aktywa odpowiada gestor. Gestor to kierownik komórki organizacyjnej Szpitala odpowiedzialny za funkcjonowanie aktywów znajdujących się na wyposażeniu komórki organizacyjnej oraz za określenie zasad dostępu i zasad akceptowalnego użycia przez pracowników. Dopuszczenie do użytkowania aktywów następuje według zasad określonych w Procedurach PR-06 QBP-01 Nadzór nad aparaturą medyczną oraz PR-05 QBP-02/E Nadzór nad sprzętem komputerowym i oprogramowaniem. Pracownicy mogą wykorzystywać aktywa Szpitala zgodnie z nich przeznaczeniem i za zgodą gestora. Pracownicy zobowiązani są do poszanowania powierzonych im aktywów oraz korzystania z nich w należyty sposób. Z chwilą rozwiązania umowy z pracownikiem gestor zobowiązany jest do rozliczenia pracownika z powierzonych mu aktywów.

Sposób wykorzystania zasobów przydzielonych do użytku prywatnego może podlegać monitorowaniu polegającego m.in. na monitorowaniu użycia komputera oraz aplikacji, śledzeniu aktywności sieciowej pracownika. Upoważnieni pracownicy Działu Informatyki mogą weryfikować wykorzystanie komputerów służbowych do realizacji zadań nie związanych bezpośrednio z pracą np. przeglądanie poczty prywatnej, korzystanie z portali społecznościowych, pobieranie nielegalnych plików. Wszystkie zasoby powierzone pracownikom nie mogą być traktowane jako zasoby prywatne.

Ze względów bezpieczeństwa teren Szpitala (wewnątrz i na zewnątrz) jest monitorowany przy użyciu kamer przez służby odpowiedzialne za ochronę obiektu. Nagrania z monitoringu mogą być użyte jako materiał dowodowy w postępowaniu wyjaśniającym. Archiwizację nagrań i nadzór nad nimi zgodnie z zawartą umową sprawuje podmiot zewnętrzny świadczący usługi z zakresu ochrony Szpitala.

3.4.8 Inwentaryzacja aktywów

Okresowo nie rzadziej niż raz na dwa lata przeprowadzana jest inwentaryzacja aktywów. Inwentaryzację aktywów należy przeprowadzać poprzez identyfikację procesów biznesowych (głównych działań) oraz aktywów biorących udział w tych procesach. Aktywa mogą być podzielone na aktywa materialne (wyposażenie, zasoby) i aktywa niematerialne (informacje, dokumenty). Każda informacja i zasób powinny mieć przypisanego właściciela informacji lub właściciela zasobu odpowiedzialnego za określenie zasad postępowania z informacją lub zasobem. Wyniki inwentaryzacji aktywów są kluczowym elementem poprawnie przeprowadzonej analizy ryzyka. Za przeprowadzanie okresowych inwentaryzacji odpowiedzialni są wyznaczeni przez Dyrektora Szpitala pracownicy. Za nadzorowanie procesu inwentaryzacji istotnych z punktu widzenia bezpieczeństwa informacji odpowiedzialny jest Pełnomocnik ds. Bezpieczeństwa. Wykaz pogrupowanych aktywów wraz z przypisanym gestorem zawarty jest w analizie ryzyka.

3.4.9 Analiza ryzyka

Głównym celem analizy ryzyka bezpieczeństwa informacji jest wyznaczenie właściwych kierunków działania kierownictwa oraz określenia priorytetów dla zarządzania zabezpieczeniami. Wyniki analizy ryzyka prowadzą do opracowania planu postępowania z ryzykiem. Poszczególne etapy analizy oraz sposób przeprowadzania analizy reguluje stosowna procedura.

3.4.10 System Kontroli dostępu

Celem podstawowym systemu zarządzania bezpieczeństwem informacji jest zapewnienie, że dostęp do informacji (która nie jest publicznie dostępna) oraz poszczególnych stref bezpieczeństwa jest możliwy tylko dla osób upoważnionych. W tym celu utworzony został plan praw dostępu. Zasady dotyczące zarządzania uprawnieniami dostępu do pomieszczeń i systemu teleinformatycznego opisane zostały w Procedurze PR-04 QBP-02 System kontroli dostępu.

3.4.11 Monitorowanie zabezpieczeń systemu zarządzania bezpieczeństwem informacji

Jedną z metod zabezpieczania aktywów Szpitala jest stosowanie zabezpieczeń mających na celu zmniejszenie ryzyka związanego ze zidentyfikowanym zagrożeniem. Skuteczność funkcjonowania

zabezpieczeń determinuje stosowanie mechanizmów okresowej kontroli i monitorowania stanu zabezpieczeń. Pełnomocnik ds. Bezpieczeństwa w porozumieniu z administratorami poszczególnych obszarów bezpieczeństwa informacji odpowiedzialny jest za zdefiniowanie miar skuteczności wybranych zabezpieczeń oraz określenie sposobu oceny tych miar. Zabezpieczenia wraz z okresami monitorowania i wyborem osób odpowiedzialnych za monitorowanie zostały określone w kartach celów. Osoby odpowiedzialne odnotowują w karcie sposób i stopień realizacji celu. Karty podlegają okresowej weryfikacji wg określonych terminów realizacji.

Monitorowanie funkcjonowania bezpieczeństwa informacji w obszarach bezpieczeństwa teleinformatycznego, fizycznego i osobowego Szpitala realizowane przez poszczególnych administratorów bezpieczeństwa odbywa się zgodnie z zasadami określonymi w Załączniku nr 5 do niniejszego dokumentu.

4. Klasyfikacja, ochrona informacji i dokumentów

Klasyfikowanie informacji ma na celu zapewnienie właściwego poziomu jej ochrony w stosunku do znaczenia informacji dla Szpitala. Tym samym możliwa jest optymalizacja nakładów związanych ze zbyt kosztowną ochroną informacji.

Klasyfikacja informacji obejmuje wszystkie informacje, z jakimi mają do czynienia pracownicy Szpitala. Dzięki poprawnie przeprowadzonej identyfikacji informacji możliwe jest zidentyfikowanie właścicieli informacji, autorów, redaktorów informacji oraz innych podmiotów współuczestniczących w przetwarzaniu informacji. Określenie grona pracowników mających dostęp do informacji, jak i określenie wagi informacji pod kątem wymagań dla integralności, dostępności i poufności pozwala na przyjęcie uzasadnionej biznesowo klasyfikacji informacji.

Klasyfikacja informacji jest jedną z form określenia sposobu postępowania z informacją i jej ochroną. Przestrzeganie klasyfikacji informacji oraz postępowanie zgodne z wytycznymi dotyczącymi klasyfikacji informacji jest kluczowe z punktu widzenia bezpieczeństwa informacji.

4.1 Ogólne zasady postępowania z informacjami i dokumentami.

Określenie klasy dokumentu powinno być dokonane na podstawie zasad klasyfikowania informacji opisanych w Załącznika nr 4 do niniejszego dokumentu. Za zarządzanie klasyfikacją informacji odpowiedzialny jest Pełnomocnik ds. Bezpieczeństwa.

Określenie klasy i jej oznaczenie musi być dokonane na jak najwcześniejszym etapie prac nad dokumentem, nie później jednak niż w chwili udostępnienia lub przekazania dokumentu innym osobom.

Autor dokumentu jest zobowiązany do określenia klasy dokumentu oraz odpowiedniego oznaczenia dokumentu lub umieszczenia go w miejscu właściwym dla klasy dokumentu w momencie tworzenia dokumentu.

Adresat dokumentu, jeśli dokument nie został dotychczas oznaczony, jest zobowiązany do określenia klasy dokumentu i odpowiedniego oznaczenia lub umiejscowienia dokumentu, właściwego dla klasy dokumentu.

Zakazana jest zmiana klasy informacji lub dokumentu bez zgody autora dokumentu. W przypadku informacji lub dokumentów „poufnych" zakazana jest również zmiana listy dostępu bez zgody autora dokumentu.

Domyślną klasą dokumentu niesklasyfikowanego (który nie jest oznaczony etykietą, nie jest umieszczony w miejscu oznaczonym etykietą) lub dokumentu, który nie jest w oczywisty sposób dokumentem poufnym (np. dokumentacja medyczna lub inna zawierająca dane osobowe), jest klasa „publicznie dostępny". Dokumenty zewnętrzne, wpływające do Szpitala nie są sklasyfikowane, dlatego adresat dokumentu po zapoznaniu się z treścią określa jego klasę.

Pracownik przekazujący lub udostępniający dokument podmiotom zewnętrznym zobowiązany jest do wyraźnego oznaczenia dokumentu adnotacją, iż jest to dokument chroniony chyba, że udostępnianie lub przekazywanie odbywa się na podstawie umowy, która stanowi inaczej lub gdy właściciel dokumentu wyrazi zgodę na udostępnienie lub przekazanie bez takiej adnotacji. Zakazane jest przekazanie dokumentu (lub informacji) innego niż dokument jawny w rozumieniu wewnętrznego regulaminu mediom bez zgody osób odpowiedzialnych za kontakty z mediami. Zgoda taka powinna mieć formę pisemną.

Informacje niebędące dokumentami (a więc nieutrwalone – np. informacje przekazywane ustnie) podlegają takiej samej ochronie jakiej podlegałyby, gdyby zostały utrwalone w formie dokumentów. W szczególności informacje sklasyfikowane jako „do użytku wewnętrznego" lub „poufne" podlegają takiej samej ochronie jak dokumenty z daną klasą informacji, zarówno przy kontaktach wewnątrz Szpitala, jak i w kontaktach z osobami spoza niego.

Każdy pracownik jest zobowiązany do niezwłocznego zgłaszania osobie upoważnionej do reagowania na incydenty, wszelkie wykryte lub podejrzewane przypadki naruszenia zasad postępowania z dokumentami. W szczególności każdy pracownik jest zobowiązany do niezwłocznego zgłaszania znalezienia dokumentu niejawnego, pozostającego bez nadzoru w miejscu nieprzeznaczonym na przechowywanie takich dokumentów.

Zasady dotyczące okresu przechowywania dokumentów oraz nadzoru nad nimi zostały określone w Procedurze PR-03 QBP-001/S Nadzór nad dokumentami i zapisami oraz Instrukcji Kancelaryjnej.