DOKUMENTACJA
ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA

TYTUŁ: PP/01 - SZBI Polityka bezpieczeństwa informacji

WŁAŚCICIEL PROCEDURY: Pełnomocnik ds. SZBI

Opracował	Sprawdził	Zatwierdził
ODO Consulting sp. z o.o., Warszawa	Barbara Tyfa – Pełnomocnik Dyrektora ds. Jakości, Bartłomiej Pałka – Kierownik Sekcji Informatyki	Dr hab. n.med. Iwona Maroszyńska prof. ICZMP – Dyrektor
Data: 13. 09. 2023 r.	Data: 13. 09. 2023 r.	Data:

I. DEKLARACJA NAJWYŻSZEGO KIEROWNICTWA

Zgodnie z treścią art. 8, 9 i 10 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Rozporządzenia Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej oraz § 20 ust. 1 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, w Instytucie „Centrum Zdrowia Matki Polki" w Łodzi (dalej „ICZMP"), ustanawia się, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali System Zarządzania Bezpieczeństwem Informacji oraz System Zarządzania Ciągłością Działania (dalej: „SZBI") zapewniające poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność oraz utrzymanie ciągłości realizacji kluczowych procesów i zadań.

SZBI będący częścią całościowego systemu zarządzania w ICZMP, oparty został na podejściu wynikającym z ryzyka i odnosi się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji oraz ciągłości działania, tj. ochrony informacji w każdym zidentyfikowanym przez ICZMP procesie jej przetwarzania oraz skutecznego zarządzania odtworzeniem kluczowych procesów na zdefiniowanym minimalnym akceptowalnym poziomie przed, w trakcie oraz po wystąpieniu sytuacji kryzysowej.

SZBI opracowany został zgodnie z obowiązującymi przepisami prawa, na podstawie Polskich Norm PN-ISO/IEC 27001 oraz PN-EN ISO 22301, a ustanowienie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich norm z rodziny ISO 27000.

Najwyższe kierownictwo ICZMP deklaruje, w szczególności:

1. zapewnienie dostępności zasobów potrzebnych do utrzymania, rozwoju i ciągłego doskonalenia SZBI,
2. zaangażowanie w odniesieniu do ustanowionego SZBI, w tym w kompleksową ochronę informacji i aktywów wspierających ich przetwarzanie oraz utrzymanie ciągłości działania ICZMP;
3. promowanie ciągłego doskonalenia ustanowionego SZBI;
4. kierowanie i aktywne wspieranie osób przyczyniających się do osiągnięcia skuteczności SZBI oraz stałe podnoszenie świadomości personelu ICZMP w zakresie bezpieczeństwa informacji i ciągłości działania.

_____

Data i podpis Dyrektora ICZMP

II. WPROWADZENIE

1. Niniejsza Polityka Bezpieczeństwa Informacji jest dokumentem głównym ustanowionego w ICZMP Systemu Zarządzania Bezpieczeństwem Informacji.

2. Dokument ma charakter deklaratywny, zawiera ogólne ramy, wymagania, zasady, procedury i instrukcje w zakresie ochrony informacji przetwarzanych w ICZMP oraz nadrzędny w stosunku do pozostałych wewnętrznych aktów prawnych dotyczących bezpieczeństwa informacji obowiązujących w ICZMP, tworząc wspólnie z nimi kompleksową dokumentację bezpieczeństwa.

3. Podstawowy wykaz skrótów i definicji stosowanych w obowiązującej dokumentacji bezpieczeństwa stanowi załącznik nr 1 do niniejszej Polityki.

4. Podstawowy wykaz aktów prawnych, polskich norm i innych dokumentów związanych z bezpieczeństwem informacji stanowi załącznik nr 2 do niniejszej Polityki.

5. Polityka Bezpieczeństwa Informacji podlega przeglądom pod kątem aktualności, przydatności i adekwatności, zgodnie z zasadami monitorowania i aktualizacji dokumentacji bezpieczeństwa określonymi w Procedurą monitorowania i nadzoru nad bezpieczeństwem informacji.

III. CELE BEZPIECZEŃSTWA INFORMACJI

1. W ICZMP ustanawia się spójne z niniejszym dokumentem, uwzględniające obowiązujące przepisy i wymagania w zakresie bezpieczeństwa informacji oraz wyniki szacowania ryzyka cele bezpieczeństwa informacji.

2. Ustanowione cele bezpieczeństwa wspierają przyjętą strategię i realizację celów ustawowych oraz strategicznych ICZMP, jak i zadań wykonywanych przez personel ICZMP, współpracowników, praktykantów, stażystów, wolontariuszy oraz inne osoby i podmioty zewnętrzne wykonujące czynności w imieniu i na rzecz ICZMP lub mające dostęp do aktywów informacyjnych ICZMP.

3. Do głównych celów bezpieczeństwa informacji w ICZMP należy:
   a) zapewnienie bezpieczeństwa aktywów informacyjnych ICZMP (w tym ochrona wizerunku i relacji z podmiotami zewnętrznymi) zgodnie z wymogami obowiązującego prawa oraz adekwatnie do wyników szacowania ryzyka w bezpieczeństwie informacji,
   b) usprawnienie funkcjonowania ICZMP poprzez uporządkowanie zasad przetwarzania informacji oraz zarządzanie aktywami informacyjnymi w zorganizowany sposób, tak aby ułatwić ciągłe doskonalenie i dostosowanie do bieżących celów ICZMP,
   c) minimalizowanie ryzyka i ograniczanie skutków utraty bezpieczeństwa informacji,
   d) stałe podnoszenie świadomości personelu oraz pozostałych osób i podmiotów, współpracujących ze ICZMP w zakresie bezpieczeństwa informacji.

4. W ramach realizacji ww. celów, adekwatnie do poziomu zidentyfikowanych zagrożeń podejmowane są działania w kierunku osiągnięcie poziomu organizacyjnego i technicznego ICZMP, który w szczególności zapewni:
   a) zachowanie poufności przetwarzanych informacji,
   b) integralność informacji oraz ich dostępność,

c) uwzględnienie dodatkowych atrybutów bezpieczeństwa zgodnie z wymaganiami i decyzjami oraz zapewnienie bezpiecznego przetwarzania informacji, w tym zdolności do podejmowania działań w sytuacjach kryzysowych,
d) udokumentowane informacje dotyczące celów bezpieczeństwa informacji i stopnia ich realizacji.

5. W ICZMP prowadzona jest okresowa ocena stopnia realizacji wyznaczonych celów bezpieczeństwa informacji. Szczegółowe zasady i tryb prowadzenia przedmiotowej oceny określa Procedura monitorowania i nadzoru nad bezpieczeństwem informacji.

IV. KONTEKST ICZMP

1. ICZMP został utworzony na podstawie Rozporządzenia Rady Ministrów z dnia 2 września 1997 r. w sprawie utworzenia Instytutu „Centrum Zdrowia Matki Polki" w Łodzi.

2. ICZMP działa na podstawie:
   1) ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych;
   2) ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym;
   3) ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej;
   4) ustawy z dnia 29 września 1994 r. o rachunkowości;
   5) ustawy z dnia 6 marca 2018 r. Prawo przedsiębiorców;
   6) ustawy z dnia 16 grudnia 2016 r. o zasadach zarządzania mieniem państwowym;
   7) statutu Instytutu „Centrum Zdrowia Matki Polki w Łodzi.

3. Działalność ICZMP ma zasięg ogólnokrajowy.

4. Nadzór nad ICZMP sprawuje Minister Zdrowia.

5. ICZMP jest państwową jednostką organizacyjną, wyodrębnioną pod względem prawnym, organizacyjnym i ekonomiczno-finansowym.

6. Instytut posiada osobowość prawną.

7. Przedmiotem działania ICZMP jest prowadzenie badań naukowych i prac rozwojowych, wdrożeniowych, szkoleń podyplomowych, uczestniczenie w systemie ochrony zdrowia ukierunkowanym na potrzeby opieki zdrowotnej.

8. Do podstawowej działalności ICZMP należy:
   1) prowadzenie badań naukowych i prac rozwojowych, w szczególności w zakresie nauk medycznych;
   2) przystosowywanie wyników badań naukowych i prac rozwojowych do potrzeb praktyki;
   3) wdrażanie wyników badań naukowych i prac rozwojowych;
   4) uczestniczenie w systemie ochrony zdrowia poprzez udzielanie świadczeń zdrowotnych, w szczególności świadczeń profilaktycznych, diagnostycznych oraz leczniczych szpitalnych i ambulatoryjnych;
   5) opiniowanie produktów kosmetycznych, preparatów biologicznych do celów medycznych, odżywczych suplementów diety, żywności dla niemowląt, środków dezynfekcyjnych do celów medycznych i weterynaryjnych, produktów mlecznych i zbożowych zawartych w tej klasie, zabawek dla dzieci, aparatury rehabilitacyjnej do ciała i diagnostycznej do celów medycznych, aparatów i instrumentów medycznych, odzieży specjalnej używanej w salach operacyjnych

lub do innych celów medycznych, bielizny osobistej i rajstop, produktów spożywczych i przemysłowych, rekomendowanych pacjentom ICZMP;

6) świadczenie usług hotelarskich polegających w szczególności na:
   a) zapewnieniu miejsc hotelowych dla pracowników zatrudnionych w ICZMP;
   b) prowadzeniu działalności hotelarskiej dla gości z zewnątrz oraz dla rodziców i opiekunów dzieci, którym ICZMP udziela świadczeń zdrowotnych;
   c) prowadzeniu innej działalności usługowej i handlowej.

9. Strukturę organizacyjną Instytutu określa regulamin organizacyjny ustalany przez Dyrektora ICZMP, po zasięgnięciu opinii rady naukowej oraz zakładowych organizacji związkowych.

10. ICZMP działający w formie instytutu badawczego stanowi podmiot leczniczy, o którym mowa w art. 4 ust. 1 pkt 4 ustawy o działalności leczniczej

11. ICZMP decyzją Ministra Zdrowia z dnia 19 lipca 2022 r. został uznany za operatora usługi kluczowej w sektorze ochrony zdrowia, polegającej na:
    1) udzielaniu świadczeń opieki zdrowotnej przez podmiot leczniczy,
    2) obrocie i dystrybucji produktów leczniczych.

12. ICZMP świadczy usługi kluczowe, o których mowa w załączniku do rozporządzenia „Wykaz usług kluczowych oraz progi istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych" polegające na udzielaniu świadczeń opieki zdrowotnej przez podmiot leczniczy oraz obrocie i dystrybucji produktów leczniczych.

13. ICZMP, jako operator usługi kluczowej, jest zobowiązany do zapewnienia niezakłócone działania systemów informacyjnych, z uwagi na zapewnienie wykonywania świadczeń zdrowotnych w sposób zapewniający kompleksowe ich udzielanie, jak i bezpieczeństwo zdrowotne pacjentów.

14. Udzielanie świadczeń opieki zdrowotnej przez ICZMP uzależnione jest od działania systemów teleinformatycznych funkcjonujących w strukturze ICZMP lub powiązanych z jego systemami. Działanie tych systemów powinno być niezakłócone, aby udzielanie świadczeń zdrowotnych mogło przebiegać w sposób prawidłowy.

15. Zgodnie z art. 95 ust. 1b pkt 1 ustawy z dnia 6 września 2001 r. Prawo farmaceutyczne – apteka, będąca w strukturze ICZMP, jest zobowiązana do przekazywania do Zintegrowanego Systemu Monitorowania Obrotu Produktami Leczniczymi, informacji o przeprowadzonych transakcjach, stanach magazynowych i przesunięciach magazynowych do innych aptek, punktów aptecznych lub działów farmacji szpitalnej produktów leczniczych. Zintegrowany System Monitorowania Obrotu Produktami Leczniczymi (ZSMOPL) to system teleinformatyczny, którego zadaniem jest przetwarzanie danych związanych z obrotem produktami leczniczymi.

16. Interesariuszami ICZMP są w szczególności:
    1) pacjenci ICZMP;
    2) pracownicy ICZMP;
    3) dostawcy, kontrahenci i inne osoby oraz podmioty realizujące zadania w imieniu i na rzecz ICZMP;
    4) Minister Zdrowia;
    5) Narodowy Fundusz Zdrowia;
    6) Prezes Urzędu Ochrony Danych Osobowych;
    7) CSIRT NASK;

8) podmioty biorące udział w ogłaszanych i przeprowadzanych przez ICZMP naborach wniosków na realizację projektów;
9) podmioty, które zawarły umowę z ICZMP na realizację i dofinansowanie projektu (beneficjenci);
10) inne niż ww. organy administracji publicznej;
11) media.

17. ICZMP funkcjonuje oraz realizuje swoje zadania z uwzględnieniem określonych uwarunkowań zewnętrznych, jak i wewnętrznych.

18. W uwarunkowań zewnętrznych, uwzględnia się w szczególności:
    1) obowiązujący porządek prawny i konieczność zapewnienie zgodności z obowiązującymi przepisami prawa,
    2) uwarunkowania ekonomiczne (w tym wpływy z podatków), technologiczne, naturalne, kulturowe, społeczne, polityczne,
    3) kluczowe czynniki i trendy zewnętrzne mające wpływ na osiągniecie celów strategicznych ICZMP,
    4) relacje i kontakty z zewnętrznymi podmiotami publicznymi i prywatnymi (w tym umowy z kontrahentami i dostawcami),
    5) wizerunek ICZMP.

19. W ramach uwarunkowań wewnętrznych, uwzględnia się w szczególności:
    1) strukturę organizacyjną ICZMP, podział kompetencji, ustanowione role i odpowiedzialności,
    2) strategie, główne cele i kierunki działania i rozwoju, zapisy wewnętrznych aktów prawnych (w tym dokumentacji bezpieczeństwa),
    3) charakter wykonywanych zadań i procesów,
    4) zasoby wykorzystywane do skutecznej realizacji powierzonych zadań i procesów (m.in. budżet, wiedza, pracownicy, budynki i pomieszczenia ICZMP, systemy informatyczne),
    5) relacje wewnętrzne i komunikację w ICZMP (m.in. przepływ informacji w formie tradycyjnej i za pośrednictwem systemu elektronicznego obiegu dokumentów),
    6) przyjęte normy, wytyczne i standardy.

20. Kontekst funkcjonowania ICZMP jest szczegółowo analizowany, poddawany ocenie i aktualizowany w ramach systemu kontroli zarządczej, w tym prowadzonego monitorowania i doskonalenia SZBI.

V. ZAKRES SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

1. Zakres ustanowionego SZBI obejmuje:
    1) procesy oraz realizowane w ICZMP działania i zadania,
    2) wszelkie informacje przetwarzane w ramach ww. procesów i zadań, w tym:
        a) przetwarzane w formie tradycyjnej (m.in. informacje wydrukowane lub zapisane na papierze),
        b) przetwarzane w formie elektronicznej (np. w elektronicznej dokumentacji medycznej, przesyłane za pośrednictwem poczty elektronicznej lub urządzeń elektronicznych, elektronicznych nośników informacji),
        c) wypowiadane słownie,

d) będące własnością ICZMP lub stron zainteresowanych, o ile zostały przekazane na podstawie obowiązujących przepisów prawnych lub umów.

3) aktywa wspierające przetwarzanie informacji w ramach ww. procesów oraz realizowanych w ICZMP działań i zadań, w tym:
   a) personel (wszyscy pracownicy ICZMP bez względu na podstawę zatrudnienia, praktykanci, stażyści, wolontariusze oraz inne osoby i podmioty zewnętrzne wykonujące czynności w imieniu i na rzecz ICZMP lub mające dostęp do aktywów informacyjnych ICZMP),
   b) budynki i pomieszczenia ICZMP, w których są lub będą przetwarzane informacje,
   c) sprzęt, w tym sprzęt komputerowy, urządzenia mobilne oraz inne nośniki danych, na których znajdują się informacje podlegające ochronie, oprogramowanie, infrastruktura sieciowa,
   d) technologie służące pozyskiwaniu, selekcjonowaniu, analizowaniu, przetwarzaniu, zarządzaniu i udostępnianiu informacji, do których zalicza się zarówno systemy papierowe jak i elektroniczne wspomagające realizację zadań publicznych,
   e) struktura organizacyjna (wszystkie komórki organizacyjne wskazane w Regulaminie Organizacyjnym ICZMP).

2. Z uwagi na szczególny charakter informacji niejawnych wynikający z obowiązujących przepisów prawa, ochrona informacji niejawnych i aktywów wspierających ich przetwarzanie podlega wyłączeniu z ustanowionego SZBI. Zasady i tryb ochrony informacji niejawnych w ICZMP określone zostały w treści odrębnych uregulowań wewnętrznych.

VI. Podstawowe zasady bezpieczeństwa informacji

1. Dążąc do możliwe jak najlepszego zabezpieczenia informacji i aktywów wspierających ich przetwarzanie wprowadza się do stosowania podstawowe zasady bezpieczeństwa informacji:
   1) **zasada „adekwatności zabezpieczeń"** – stosowane zabezpieczenia muszą być adekwatne do zidentyfikowanych zagrożeń,
   2) **zasada „bezpiecznego przetwarzania"** – przetwarzanie informacji szczególnie chronionych powinno odbywać się wyłącznie w bezpiecznych środowiskach, tj. w wydzielonych systemach informatycznych, zabezpieczonych pomieszczeniach etc.,
   3) **zasada „bezpiecznej współpracy z podmiotami zewnętrznymi"** – dokumenty regulujące współpracę z podmiotami zewnętrznymi (m.in. treść umów i porozumień) zawierają zapisy dot. bezpieczeństwa informacji, w tym klauzule bezpieczeństwa o zachowaniu poufności,
   4) **zasada „czystego biurka** – w celu wyeliminowania ryzyka przypadkowego lub celowego odczytania informacji, ich skopiowania, zniszczenia lub zmodyfikowania przez osoby nieuprawnione, opuszczając stanowisko pracy należy usunąć z blatu biurka dokumenty zawierające informacje inne niż informacje o charakterze jawnym, umieszczając je w przeznaczonych do tego celu zabezpieczonych meblach biurowych: szafach, szufladach lub sejfach,
   5) **zasada „czystego ekranu"** – na czas nieobecności dostęp do komputera należy skutecznie blokować a po zakończeniu pracy komputer wyłączyć, chyba że musi on pracować w trybie ciągłym,
   6) **zasada „doskonalenia SZBI"** – system zarządzania bezpieczeństwem informacji jest dostosowywany do zmieniających się warunków w oparciu o wyniki okresowo prowadzonego monitorowania i nadzoru,
   7) **zasada „segregacji obowiązków i zadań"** – obowiązki i uprawnienia powinny być tak rozdzielone, aby pojedyncza osoba nie dysponowała pełnią uprawnień do wykonywania zadań w całości,

8) **zasada „uprawnionego dostępu"** – korzystanie z aktywów informacyjnych ICZMPa odbywać się może tylko w oparciu o formalne uprawnienia do korzystania z wybranych aktywów,
9) **zasada „wiedzy uzasadnionej"** – personel ICZMPa dysponuje wiedzą o aktywach informacyjnych w ograniczonym zakresie, niezbędnym do realizacji powierzonych im zadań.

2. Dodatkowe zasady bezpieczeństwa mogą zostać określone w pozostałych dokumentach wchodzących w skład dokumentacji bezpieczeństwa.

3. Personel ICZMP, oraz inne podmioty zewnętrzne wykonujące czynności w imieniu i na rzecz ICZMP lub mające dostęp do aktywów informacyjnych ICZMP są zobowiązani do przestrzegania obowiązujących w ICZMP zasad bezpieczeństwa.

VII. ROLE I ODPOWIEDZIALNOŚĆ W ZAKRESIE BEZPIECZEŃSTWA INFORMACJI

1. Właściwe zarządzanie bezpieczeństwem informacji w ICZMP zapewnia struktura organizacyjna, w której skład wchodzą w szczególności:
   1) Dyrektor ICZMP;
   2) Pełnomocnik ds. SZBI;
   3) Inspektor Ochrony Danych;
   4) Administratorzy systemów;
   5) Kierownik Sekcji Informatyki, będący Przewodniczącym Zespołu ds. Bezpieczeństwa Informacji;
   6) kierujący komórkami organizacyjnymi ICZMP;
   7) pozostały personel ICZMP.

2. Obowiązki i role są przydzielane w sposób zapobiegający powstaniu konfliktu pomiędzy nimi oraz zapewniający rzetelność i bezstronność wykonywania zadań związanych z bezpieczeństwem informacji.

3. Dyrektor ICZMP:
   1) zapewnia zasoby niezbędne do prawidłowego funkcjonowania SZBI;
   2) podejmuje strategiczne decyzje w procesie zarządzania bezpieczeństwem informacji;
   3) wyznacza Inspektora Ochrony Danych;
   4) powołuje Pełnomocnika ds. SZBI;
   5) zatwierdza dokumentację SZBI oraz jej zmiany;
   6) kieruje i wspiera osoby przyczyniające się do osiągnięcia skuteczności SZBI;
   7) promuje ciągłe doskonalenie SZBI.

4. Pełnomocnik ds. SZBI:
   1) odpowiada za zapewnienie zgodności SZBI z właściwymi wymaganiami, w szczególności z wymaganiami norm: PN-EN ISO/IEC 27001 i PN-ISO/IEC 22301;
   2) inicjuje oraz nadzoruje działania wdrożeniowe, korygujące i zapobiegawcze w zakresie bezpieczeństwa informacji;
   3) koordynuje proces zarządzania ryzykiem bezpieczeństwa informacji;
   4) nadzoruje opracowanie, przeglądy i aktualizacje dokumentacji SZBI;
   5) opracowuje i przeprowadza szkolenia z zakresu SZBI;
   6) nadzoruje proces zarządzania incydentami bezpieczeństwa;

7) nadzoruje lub prowadzi audyty SZBI oraz okresowy przegląd SZBI;
8) prowadzi rejestr aktywów;
9) wydaje opinie, zalecenia oraz rekomendacje w zakresie związanym z funkcjonowaniem SZBI;
10) odpowiada za utrzymywanie kontaktów z grupami zainteresowanych specjalistów lub innymi specjalistycznymi forami oraz stowarzyszeniami zawodowymi z obszaru bezpieczeństwa informacji;
11) podejmuje działania w pozostałych kwestiach związanych z bezpieczeństwem informacji, w zakresie niezastrzeżonym do kompetencji innych osób.

5. Inspektor Ochrony Danych (IOD) odpowiada za monitorowanie i zapewnienie przestrzegania przepisów o ochronie danych osobowych w ICZMP, w szczególności Rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: RODO). Szczegółowe obowiązki oraz uprawnienia Inspektora Ochrony Danych określa Polityka ochrony danych osobowych.

6. Administratorzy Systemów odpowiadają za zarządzanie systemami teleinformatycznymi ICZMP. Szczegółowe obowiązki oraz uprawnienia Administratorów Systemów określa Procedura użytkowania sieci teleinformatycznej.

7. Kierujący Komórkami organizacyjnymi ICZMP:
   1) nadzorują realizację obowiązków wynikających z SZBI przez podległy im personel ICZMP;
   2) identyfikują aktywa oraz dokonują oceny ich krytyczności oraz klasyfikacji;
   3) dokonują oceny ryzyka bezpieczeństwa informacji w podlegających im obszarach;
   4) współpracują z Pełnomocnikiem ds. SZBI, Inspektorem Ochrony Danych oraz Administratorem Systemu, w ramach realizowanych przez nich zadań;
   5) zarządzają ciągłością działania w podlegających im obszarach.

8. Personel ICZMP:
   1) realizuje obowiązki wynikające z SZBI w zakresie powierzonych im zadań;
   2) informuje niezwłocznie o wszystkich zdarzeniach mających wpływ na ryzyko bezpieczeństwa informacji, w tym w szczególności o incydentach bezpieczeństwa;
   3) współpracuje z Pełnomocnikiem ds. SZBI, Inspektorem Ochrony Danych oraz Administratorem Systemu w ramach realizowanych przez nich zadań;
   4) odbywa obowiązkowe szkolenia z zakresu SZBI.

9. Centralny Zespół ds. Reagowania na Incydenty odpowiada za zapewnienie obsługi incydentu zgodnie z Procedurą zarządzania incydentem.

10. Zespół ds. Zarządzania Ciągłością Działania odpowiada za koordynowanie działań organizacji zarówno w trakcie wystąpienia zakłócenia, jak i w warunkach bieżącej działalności organizacji. Zespół odpowiada także za aktualność wszystkich ustanowionych Planów Ciągłości Działania w tym uczestniczy w przeglądzie zarządzania SZCD.

11. Zespół ds. cyberbezpieczeństwa odpowiada za:
   1) identyfikowanie zagrożeń w odniesieniu do systemów informacyjnych ICZMP oraz proponowanie rozwiązań ograniczających ryzyko wynikające z tych zagrożeń,
   2) analizowanie oprogramowania szkodliwego i określanie jego wpływu na system informacyjny ICZMP;

3) wykrywanie przełamania lub ominięcia zabezpieczeń systemu informacyjnego ICZMP, prowadzenie analizy powłamaniowej wraz z określeniem działań niezbędnych do przywrócenia sprawności systemu informacyjnego ICZMP,
4) zabezpieczanie informacji potrzebnych do analizy powłamaniowej, pozwalających na określenie wpływu incydentu poważnego na świadczenie usługi kluczowej.

12. Pełnomocnikiem ds. SZBI może być osoba, która:
    1) posiada właściwe kwalifikacje zawodowe, a w szczególności wiedzę fachową nt. zasad bezpieczeństwa informacji lub zarządzania systemem teleinformatycznym oraz umiejętności wypełnienia zadań określonych niniejszym rozdziale;
    2) posiada co najmniej dwuletnie doświadczenie w zakresie zarządzania bezpieczeństwem informacji lub systemem teleinformatycznym.

VIII. KLASYFIKACJA PRZETWARZANYCH INFORMACJI

1. Informacje przetwarzane w ICZMP objęte zakresem ustanowionego SZBI klasyfikowane są w następujących grupach:
    1) dane osobowe (w rozumieniu przepisów RODO),
    2) tajemnice prawnie chronione (tajemnice powołane na mocy ustaw, których obowiązek ochrony wynika z tychże ustaw),
    3) tajemnice ICZMP (informacje, których ujawnienie mogłoby narazić ICZMP na szkodę oraz informacje wewnętrzne udostępniane na zasadzie „wiedzy uzasadnionej"),
    4) informacje jawne (w tym informacje udostępniane w trybie informacji publicznej).

2. Szczegółowe zasady dotyczące bezpieczeństwa i ochrony poszczególnych grup informacji, w tym ich zakres, tryb udostępniania lub dystrybucji oraz archiwizacji i niszczenia zostały określone w dedykowanych procedurach bezpieczeństwa.

IX. STRUKTURA DOKUMENTACJI

1. Dokumentacja określona w SZBI dzieli się na dwie podstawowe klasy: dokumentację normatywną i dokumentację operacyjną.

2. Dokumentację normatywną stanowią przepisy prawa powszechnego oraz wewnętrzne akty normatywne wydawane przez Dyrektora ICZMP w postaci zarządzeń, decyzji i poleceń służbowych.

3. Drugą z klas dokumentacji jest dokumentacja operacyjna, sporządzana w ramach prowadzenia bieżącej działalności ICZMP, a w szczególności dokumentacja w postaci zapisów z wykonanych czynności, stanowiąca ślad audytowy, na podstawie którego można stwierdzić prawidłowość wykonywania nałożonych obowiązków.

4. Dokumenty poświadczające każdorazowe wykonanie procedur wynikających z SZBI mogą być prowadzone w postaci papierowej lub elektronicznej, zależnie od okoliczności.

5. W ramach ustanowionego SZBI wprowadza się trójpoziomową dokumentację bezpieczeństwa określającą zasady i tryb zarządzania bezpieczeństwem informacji oraz aktywów wspierających przedmiotowe przetwarzanie w ICZMP:

1) w ramach I poziomu SZBI (dokumenty o charakterze publicznym, ogólnodostępnym) wyróżnia się Politykę Bezpieczeństwa Informacji, która:
   - stanowi dokument nadrzędny w stosunku do pozostałych wewnętrznych aktów prawnych dotyczących bezpieczeństwa informacji obowiązujących w ICZMP, tworzących wspólnie dokumentację bezpieczeństwa,
   - określa ogólne ramy, kierunki, zasady i wymogi bezpieczeństwa informacji w ICZMP oraz zakres dokumentacji bezpieczeństwa na pozostałych poziomach,
   - jest wprowadzana i aktualizowana w formie zarządzenia Dyrektora ICZMP.

2) W ramach II poziomu SZBI (dokumenty dedykowane i udostępniane całemu personelowi ICZMP, w uzasadnionych przypadkach wybranym osobom i podmiotom zewnętrznym wykonującym czynności w imieniu i na rzecz ICZMP lub mającym dostęp do aktywów informacyjnych ICZMP) wyróżnia się dedykowane polityki tematyczne:
   a) zawierające uszczegółowienie zapisów polityki I poziomu SZBI,
   b) określające specyficzne wymogi i zasady bezpieczeństwa w kluczowych obszarach bezpieczeństwa informacji:
      - procedury bezpieczeństwa dedykowane dla poszczególnych grup informacji wskazanych w rozdziale VIII niniejszej Polityki,
      - procedura zarządzania aktywami informacyjnymi,
      - procedura zarządzania ryzykiem,
      - procedura zarządzania incydentem,
      - procedura użytkowania sieci teleinformatycznej,
      - procedura bezpieczeństwa fizycznego i środowiskowego,
      - procedura zarządzania ciągłością działania,
      - procedura bezpieczeństwa w relacjach z podmiotami zewnętrznymi,
      - procedura zarządzania incydentami,
      - procedura monitorowania i nadzoru nad bezpieczeństwem informacji,
   c) wprowadzane i aktualizowane w formie załączników do polityki I poziomu SZBI lub na mocy odrębnych zarządzeń, decyzji i poleceń służbowych Dyrektora ICZMP.

3) W ramach III poziomu SZBI (dokumenty dedykowane i udostępniane wybranym osobom i podmiotom na zasadzie „wiedzy uzasadnionej") wyróżnia się:
   a) wybrane procedury i instrukcje wykonawcze:
   b) określające zasady i sposób realizacji wymogów w obszarach uregulowanych na II poziomie SZBI w danej komórce organizacyjnej lub przez dany podmiot zewnętrzny wykonujący czynności w imieniu i na rzecz ICZMP,
   c) wprowadzane i aktualizowane w formie załączników do dokumentów II poziomu SZBI lub dokumentów wewnętrznych wybranych komórek organizacyjnych ICZMP, ewentualnie na mocy odrębnych zarządzeń, decyzji lub poleceń służbowych Dyrektora ICZMP,
   d) instrukcje lub procedury bezpieczeństwa dla wybranych komórek organizacyjnych w związku z realizacją projektów unijnych,
   e) wybrane umowy ze stronami trzecimi.

2. Dokumenty opracowywane na poszczególnych poziomach SZBI uzupełniają się wzajemnie, tworząc kompleksową dokumentację Systemu Zarządzania Bezpieczeństwem Informacji w ICZMP (dokumentację bezpieczeństwa):
   1) dokumentacja I poziomu SZBI ma charakter ogólny, a jej zapisy odwołują się wprost do dedykowanych dokumentów II poziomu SZBI, w których przedmiotowe zapisy są uszczegółowione,

2) poszczególne dokumenty II poziomu SZBI odwołują się do siebie oraz do procedur lub instrukcji III poziomu SZBI,
3) procedury lub instrukcje III poziomu SZBI uszczegółowiają wybrane kwestie zidentyfikowane w ramach dokumentacji II poziomu.

3. W przyjętym w ICZMP modelu bezpieczeństwa dopuszcza się opracowywanie dodatkowych dokumentów dot. bezpieczeństwa informacji, w tym regulaminów, rekomendacji, zasad, wytycznych.

4. Celem zapewnienia właściwości, adekwatności i skuteczności obowiązujących przepisów wewnętrznych w zakresie bezpieczeństwa, prowadzone są okresowe przeglądy i aktualizacja ww. dokumentacji. Zasady oraz tryb prowadzenia przedmiotowych przeglądów dokumentacji SZBI uregulowano w Procedurze monitorowania i nadzoru nad bezpieczeństwem informacji.

X. KONTROLA DOSTĘPU DO INFORMACJI

1. W ramach zapewnienia ograniczonego dostępu do aktywów informacyjnych ICZMP, w tym do budynków i pomieszczeń, sprzętu i urządzeń oraz systemów informatycznym tylko dla osób i podmiotów uprawnionych, prowadzona jest kontrola dostępu fizycznego i logicznego.
2. Szczegółowe zasady zarządzania dostępem do aktywów informacyjnych ICZMP zostały uregulowane w Polityce bezpieczeństwa fizycznego i środowiskowego oraz dedykowanych procedurach III poziomu SZBI.

XI. ZARZĄDZANIE AKTYWAMI INFORMACYJNYMI

1. W celu zapewnienia adekwatnego poziomu bezpieczeństwa aktywów informacyjnych, przedmiotowe aktywa są inwentaryzowane, klasyfikowane i zarządzane zgodnie z obowiązującymi wymaganiami w zakresie ich ochrony.
2. Szczegółowe zasady dotyczące identyfikowania, klasyfikowania, postępowania z aktywami oraz odpowiedzialności za aktywa informacyjne zostały uregulowane w Procedurze zarządzania aktywami informacyjnymi.

XII. ZARZĄDZANIE RYZYKIEM W BEZPIECZEŃSTWIE INFORMACJI

1. Skuteczne zarządzanie bezpieczeństwem informacji wymaga podejmowania okresowych działań w obszarze zarządzania ryzykiem, w szczególności w zakresie szacowania tj. identyfikowania, analizy i oceny ryzyka w bezpieczeństwie informacji, zmierzających do ograniczenia oraz eliminacji przedmiotowego ryzyka.

2. Działania związane z zarządzaniem ryzykiem mającym wpływ na bezpieczeństwo informacji obejmują w szczególności:
   1) przygotowanie oraz okresową aktualizację dokumentów dot. zarządzania ryzykiem,
   2) prowadzenie okresowego szacowania ryzyka,
   3) postępowanie z ryzykiem,
   4) podejmowanie działań korygujących.

3. Szczegółowe zasady dot. zarządzania ryzykiem w bezpieczeństwie informacji zostały uregulowane w Procedurze zarządzania ryzykiem.

XIII. BEZPIECZEŃSTWO TELEINFORMATYCZNE

1. W ramach zarządzania bezpieczeństwem teleinformatycznym podejmowane są działania w zakresie szacowania i kontroli ryzyka utraty poufności, integralności, dostępności informacji w związku z korzystaniem z elektronicznej dokumentacji medycznej oraz aplikacji, komputerów i urządzeń mobilnych, sieci komputerowych i transmisji danych.

2. Przedmiotowe działania podejmowane są w szczególności w zakresie rozwoju, monitorowania i doskonalenia infrastruktury teleinformatycznej.

3. Szczegółowe zasady i wymogi w zakresie bezpieczeństwa teleinformatycznego zostały uregulowane w Procedurze użytkowania sieci teleinformatycznej, oraz dedykowanych procedurach i instrukcjach III poziomu SZBI.

XIV. BEZPIECZEŃSTWO FIZYCZNE I ŚRODOWISKOWE

1. W celu zapobieżenia nieuprawnionemu fizycznemu dostępowi, szkodom i zakłóceniom w przetwarzaniu informacji i środkach przetwarzania informacji oraz utracie, zniszczeniu, uszkodzeniu, kradzieży aktywów informacyjnych ICZMP stosowane są mechanizmy ochrony w obszarze bezpieczeństwa fizycznego i środowiskowego.

2. Szczegółowe zasady dot. zarządzania bezpieczeństwem fizycznym i środowiskowym zostały uregulowane w Procedurze bezpieczeństwa fizycznego i środowiskowego, oraz dedykowanych procedurach i instrukcjach, w tym procedurach III poziomu SZBI.

XV. BEZPIECZEŃSTWO ZASOBÓW LUDZKICH

1. Celem ograniczenia ryzyka błędu ludzkiego, kradzieży lub nadużycia oraz zapewnienia, że personel ICZMP oraz inne osoby lub podmioty wykonujące czynności w imieniu i na rzecz ICZMP lub mające dostęp do aktywów informacyjnych ICZMP są świadomi odpowiedzialności i swoich obowiązków dotyczących bezpieczeństwa informacji oraz wypełniają je w odpowiedni sposób i z uwzględnieniem interesów ICZMP, podejmowane są określone działania w obszarze bezpieczeństwa zasobów ludzkich, w szczególności:
   1) zapewnienie wykwalifikowanych pracowników lub innych osób oraz podmiotów zewnętrznych do realizacji zadań,
   2) uwzględnienie odpowiednich zapisów dotyczących odpowiedzialności w zakresie bezpieczeństwa informacji w umowach zawieranych z ww. osobami i podmiotami,
   3) szkolenie ww. osób i podmiotów w zakresie bezpieczeństwa informacji oraz regularne informowanie o aktualizacji polityk i procedur związanych z ich stanowiskiem pracy.

2. Szczegółowe zasady dotyczące zarządzania bezpieczeństwem zasobów ludzkich zostały uregulowane w dedykowanych procedurach, regulaminach (w szczególności regulaminie

dotyczącym procesu rekrutacji) i instrukcjach, w tym procedurach III poziomu SZBI, w szczególności w Procedurze zarządzania bezpieczeństwem osobowym.

XVI. ZAPEWNIENIE CIĄGŁOŚCI DZIAŁANIA

1. W ICZMP podejmowane są działania w zakresie planowania, weryfikowania, zapewnienia, przeglądu i oceny ciągłości działania i postępowania w przypadku wystąpienia sytuacji kryzysowych.

2. Szczegółowe zasady dot. zarządzania ciągłością działania zostały uregulowane w Polityce zarządzania ciągłością działania oraz dedykowanych procedurach i instrukcjach, w tym procedurach III poziomu SZBI.

XVII. RELACJE Z PODMIOTAMI ZEWNĘTRZNYMI

1. Celem zapewnienia ochrony aktywów informacyjnych udostępnianych usługodawcom, dostawcom i innym osobom lub podmiotom zewnętrznym wykonującym czynności w imieniu i na rzecz ICZMP lub mającym dostęp do aktywów ICZMP, wprowadza się zasady postępowania w przypadku współpracy związanej z dostępem do aktywów informacyjnych ICZMP i korzystania z usług ww. osób i podmiotów.

2. W przypadku wykonywania zadań delegowanych lub korzystania z aktywów, w tym przetwarzania informacji powierzonych przez podmioty zewnętrzne w drodze stosownej umowy lub porozumienia, poza wymogami określonymi w obowiązującej w ICZMP dokumentacji bezpieczeństwa dopuszcza się stosowanie wymogów i zaleceń bezpieczeństwa określonych przez ww. podmioty zewnętrzne, o ile wskazane wymogi i zalecenia zewnętrzne nie obniżają poziomu bezpieczeństwa pozostałych informacji przetwarzanych w ICZMP.

3. Przedmiotowe zasady i wymogi współpracy zostały uregulowane w Procedurach bezpieczeństwa w relacjach z podmiotami zewnętrznymi.

XVIII. ZGODNOŚĆ Z PRZEPISAMI PRAWA I ZAPISAMI UMÓWNYMI

1. W celu uniknięcia naruszenia obowiązujących przepisów prawa, zobowiązań ustawowych, zapisów zawartych umów i porozumień, w ICZMP prowadzona jest bieżąca kontrola zgodności regulacji wewnętrznych, przyjętych zasad bezpieczeństwa i ich stosowania z ww. przepisami, w tym identyfikowanie, dokumentowanie i aktualizowanie wszystkich istotnych wymagań prawnych, regulacyjnych, umownych oraz podejścia organizacji do ich przestrzegania.

2. Przedmiotowa kontrola dotyczy również zgodności z wymaganiami prawnymi, regulacyjnymi i umownymi, związanymi z prawami własności intelektualnej i użytkowaniem prawnie zastrzeżonego oprogramowania.

3. Kierownicy komórek organizacyjnych, w zakresie zadań realizowanych zgodnie z Regulaminem Organizacyjnym prowadzą bieżący nadzór w swoich komórkach w zakresie zgodności z przepisami prawa i zapisami umownymi.

4. Inspektor Ochrony Danych w ICZMP odpowiedzialny jest za zapewnienia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, w szczególności RODO.

5. Pełnomocnik ds. SZBI, we współpracy z kierownikami poszczególnych komórek organizacyjnych ICZMP dokonuje okresowych przeglądów regulacji wewnętrznych dotyczących bezpieczeństwa informacji w zakresie ich zgodności z przepisami prawa i zapisami umownymi, na zasadach i w trybie określonym w Procedurze monitorowania i nadzoru nad bezpieczeństwem informacji, oraz innych dedykowanych procedurach.

6. ICZMP zapewnia okresowy audyt w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

7. Polityka Bezpieczeństwa Informacji oraz opracowywane dokumenty II i III poziomu SZBI są zgodne z obowiązującymi przepisami prawa oraz wybranymi standardami międzynarodowymi dot. bezpieczeństwa informacji, w szczególności ze wskazanymi w Wykazie aktów prawnych, polskich norm i innych dokumentów związanych z bezpieczeństwem informacji.

XIX. NARUSZENIE BEZPIECZEŃSTWA INFORMACJI I ODPOWIEDZIALNOŚC Z TYTUŁU NARUSZENIA

1. Podstawową konsekwencją naruszenia bezpieczeństwa informacji jest obniżenie poziomu ochrony przetwarzanych informacji i aktywów wspierających ich przetwarzanie w ICZMP.

2. Każdy, kto posiada dostęp do informacji i aktywów wspierających ich przetwarzanie w ICZMP (personel ICZMP, jak również podmioty zewnętrzne wykonujące czynności w imieniu i na rzecz ICZMP lub mające dostęp do aktywów informacyjnych ICZMP) ma obowiązek informowania podmioty odpowiedzialne za bezpieczeństwo przetwarzania informacji w ICZMP o podejrzeniu lub każdym zidentyfikowanym przypadku naruszenia bezpieczeństwa informacji.

3. Nieprzestrzeganie zasad zawartych w dokumentacji bezpieczeństwa stanowi naruszenie obowiązków pracowniczych i może skutkować pociągnięciem personelu ICZMP do odpowiedzialności dyscyplinarnej.

4. Naruszenie postanowień niniejszej Polityki przez kontrahenta ICZMP lub jego pracowników stanowi podstawę do odstąpienia od umowy i żądania pokrycia powstałej szkody lub zapłaty kary umownej, jeżeli taki obowiązek wynika z zawartej umowy.

5. Z tytułu działań personelu lub kontrahentów ICZMP lub innych osób i podmiotów niezgodnych z przepisami prawa powszechnie obowiązującego (w szczególności dot. przetwarzania danych osobowych), grożą odrębne kary określone w szczególności w:
   1) kodeksie pracy,
   2) kodeksie cywilnym,
   3) kodeksie karnym,
   4) ustawie o ochronie danych osobowych.

6. W celu uzyskania możliwie pełnej informacji o naruszeniu bądź też podejrzeniu naruszenia bezpieczeństwa informacji w ICZMP, osoby bądź podmioty niezwiązane z ze ICZMP mogą zgłaszać przypadki bądź podejrzenie naruszenia bezpieczeństwa aktywów informacyjnych ICZMP na adres incydent@iczmp.edu.pl.

7. Szczegółowe zasady dot. identyfikowania, zgłaszania, reagowania i obsługi zdarzeń i incydentów związanych z bezpieczeństwem informacji zostały uregulowane w Procedurze zarządzania incydentem.

XX. DOBÓR ZABEZPIECZEŃ

1. Cele i dobór zabezpieczeń w SZBI prowadzony jest w oparciu o aktualne wymogi prawa powszechnie obowiązującego, zalecenia polskiej normy ISO 27000 oraz wyniki monitorowania Systemu, w szczególności wyniki szacowania ryzyka w bezpieczeństwie informacji.

2. Stosowane zabezpieczenia fizyczne, techniczne i organizacyjne powinny uzupełniać się wzajemnie, zapewniając wymagany poziom bezpieczeństwa informacji.

3. Wykaz stosowanych zabezpieczeń wraz z celami ich stosowania i uzasadnieniem ich wyboru lub wyłączenia ma charakter udokumentowanej informacji, opracowanej w formie Deklaracji Stosowania zawartej w niniejszej Polityce.

XXI. UTRZYMYWYWANIE, MONITOROWANIE I DOSKONALENIE SZBI

1. Działania w zakresie utrzymania, monitorowania i doskonalenia SZBI podejmowane są w szczególności w zidentyfikowanych na II poziomie SZBI obszarach bezpieczeństwa.

2. Działania, o których mowa w ust. 1 mają charakter działań bieżących i okresowych.

3. W oparciu o wyniki prowadzonego monitorowania i nadzoru nad bezpieczeństwem informacji, w przypadku zidentyfikowania niezgodności podejmowane są adekwatne działania doskonalące, w tym działania korygujące mające na celu wyeliminowanie przyczyn niezgodności.

4. W ICZMP prowadzone jest ciągłe doskonalenie przydatności, adekwatności i skuteczności ustanowionego systemu zarządzania bezpieczeństwem informacji.

5. Szczegółowe zasady dot. monitorowania i doskonalenia SZBI zostały określone w Procedurze działań korygujących i doskonalących oraz Procedurze monitorowania i nadzoru nad bezpieczeństwem informacji oraz innych dedykowanych procedurach.

XXII. INFORMOWANIE O TREŚCI DOKUMENTACJI BEZPIECZEŃSTWA

1. Niniejszy dokument Polityki wraz z załącznikami mają charakter jawny i są ogólnodostępne.

2. Dokumenty powiązane, w tym zawierające dokumentację II poziomu SZBI udostępniane są całemu personelowi ICZMP, a w uzasadnionych przypadkach wybranym osobom lub podmiotom zewnętrznym wykonującym czynności w imieniu i na rzecz ICZMP lub mającym dostęp do aktywów informacyjnych ICZMP.

3. Dokumentacja III poziomu SZBI udostępniana jest w ograniczonym zakresie, wybranym pracownikom lub innym osobom i podmiotom zewnętrznym na zasadzie „wiedzy uzasadnionej", pozwalającym na realizację powierzonych zadań.

XXIII. ZAŁĄCZNIK:

1. Załącznik nr 1 do Polityki PP/01 – SZBI - Wykaz skrótów i definicji;
2. Załącznik nr 2 do Polityki PP/01 – SZBI - Wykaz aktów prawnych, polskich norm i innych dokumentów związanych z bezpieczeństwem informacji.

XXIV. DOKUMENTY ZWIĄZANE:

1. PP/02 – SZBI - Polityka ochrony danych osobowych;
2. PP/03 – SZBI - Polityka ciągłości działania;
3. PP/04 – SZBI - Procedura nadawania upoważnień;
4. PP/05 – SZBI - Procedura udostępniania danych;
5. PP/06 – SZBI - Procedura powierzenia przetwarzania danych;
6. PP/07 – SZBI - Procedura oceny skutków;
7. PP/08 – SZBI - Procedura zarządzania ryzykiem bezpieczeństwa informacji;
8. PP/09 – SZBI - Procedura zarządzania podatnościami;
9. PP/10 – SZBI - Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji;
10. PP/11 – SZBI - Procedura użytkowania sieci teleinformatycznej;
11. PP/12 – SZBI - Procedura rejestracji i inwentaryzacji oprogramowania i sprzętu komputerowego;
12. PP/13 – SZBI - Procedura pracy zdalnej;
13. PP/14 – SZBI - Procedura dostępu VPN do zasobów sieci ICZMP;
14. PP/15 – SZBI - Procedura przechowywania i przekazywania hasła administratora systemu;
15. PP/16 – SZBI - Procedura wykonywania kopii zapasowych;
16. PP/17 – SZBI - Procedura rejestracji i inwentaryzacji sprzętu medycznego;
17. PP/18 – SZBI - Procedura zarządzania zmianą IT;
18. PP/19 – SZBI - Procedura privacy by design, privacy by default;
19. PP/20 – SZBI - Procedura zarządzania aktywami informacyjnymi;
20. PP/21 – SZBI - Procedura zarządzania bezpieczeństwem zasobów ludzkich;
21. PP/22 – SZBI - Procedura bezpieczeństwa fizycznego i środowiskowego;
22. PP/23 – SZBI - Procedura zarządzania kluczami;
23. PP/24 – SZBI - Procedura zarządzania uprawnieniami w systemie kontroli dostępu;
24. PP/25 – SZBI - Procedura dostępu do serwerowni;
25. PP/26 – SZBI - Procedura zarządzania systemem monitoringu wizyjnego;
26. PP/27 – SZBI - Procedura korzystania z bezprzewodowej sieci dla pracownika;
27. PP/28 – SZBI - Procedura korzystania z bezprzewodowej sieci dla gości;
28. PP/29 – SZBI - Procedura bezpieczeństwa w relacjach z podmiotami zewnętrznymi dla pracowników;
29. PP/30 – SZBI - Procedura bezpieczeństwa w relacjach z podmiotami zewnętrznymi dla dostawców;
30. PP/31 – SZBI - Procedura monitorowania i nadzoru nad bezpieczeństwem informacji.

Załącznik nr 1 do Polityki PP/01 – SZBI - **Wykaz skrótów i definicji**

Pojęcie	Definicja
Adekwatność (minimalizacja danych)	zasada dotycząca przetwarzania informacji polegająca na tym, że administrator danych powinien przetwarzać tylko takiego rodzaju dane i tylko o takiej treści, które są niezbędne do realizacji celu dla którego dane są zbierane;
Administrator	osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. W niniejszej dokumentacji ochrony danych osobowych przez administratora danych rozumie się ICZMP;
Administrator Systemu	pracownik ICZMP zarządzający prawami dostępu do systemów oraz usług w sieci teleinformatycznej ICZMP;
Aktywa	wszystko, co ma wartość dla ICZMP, a w szczególności: personel, wizerunek, informacje wytwarzane, przetwarzane i przechowywane w ICZMP, mienie wykorzystywane przez ICZMP oraz jej personel, i z tego powodu wymaga ochrony;
Aktywa informacyjne	kluczowe procesy i zadania, informacje przetwarzane w dowolnej formie, w tym papierowej i elektronicznej w ramach ww. procesów i zadań oraz aktywa wspierające przedmiotowe przetwarzanie, posiadające wartość dla ICZMP i wymagające właściwej ochrony przed utratą dostępności, poufności i integralności;
Analiza ryzka	zidentyfikowane ryzyka należy poddać analizie mającej na celu określenie prawdopodobieństwa wystąpienia danego ryzyka i możliwych jego skutków;
Anonimizacja	przekształcenie danych osobowych, po którym nie można już przyporządkować poszczególnych informacji osobistych lub rzeczowych do określonej lub możliwej do zidentyfikowania osoby fizycznej albo można tego dokonać jedynie niewspółmiernie dużym nakładem czasu, kosztów lub działań;
Audyt	systematyczny, niezależny i udokumentowany proces uzyskiwania dowodu z audytu oraz jego obiektywnej oceny w celu określenia stopnia spełnienia kryteriów audytu;
Autentyczność	właściwość, która polega na tym, że podmiot jest tym, za kogo się podaje; właściwość polegająca na tym, że pochodzenie lub zawartość danych opisujących obiekt są takie jak deklarowane (KRI);
Bezpieczeństwo informacji	zachowanie poufności, integralności i dostępności informacji; dodatkowo, mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;
Centralny Zespół ds. Reagowania na Incydenty (CZRI)	wewnętrzna struktura odpowiedzialna za cyberbezpieczeństwo w ICZMP powołana odrębnym Zarządzeniem Dyrektora ICZMP;
Ciągłość działania	zdolność ICZMP do ciągłego świadczenia usług w akceptowalnych ramach czasowych przy zdefiniowanej wcześniej zdolności do działania w czasie zakłócenia;
CMDB	Configuration Management Database - to repozytorium przechowujące informacje o komponentach tworzących infrastrukturę IT;
CSIRT NASK	Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego

	działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy;
Cyberbezpieczeństwo	odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;
Dane osobowe	informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
Deklaracja stosowania	Dokument określający, które zabezpieczenia zostały wdrożone, jakie są cele stosowania tych zabezpieczeń, wraz z uzasadnieniem ich wyboru lub wykluczenia zgodnie z normą PN-ISO/IEC 27001;
Dokumentacja bezpieczeństwa	zespół powiązanych ze sobą spójnych dokumentów określających zasady i sposoby zarządzania bezpieczeństwem informacji oraz aktywów wspierających przetwarzanie informacji w ICZMP;
Dostępność	właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu; właściwość określająca, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w założonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym (KRI);
Działania korygujące	działanie mające na celu wyeliminowanie przyczyny określonego stanu rzeczy (niezgodności) i zapobieżenie jego powtórzeniu;
Działania naprawcze	działanie podejmowane w celu wyeliminowania określonego stanu rzeczy i przywrócenia stanu pożądanego;
Działa zaradcze	środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym środki w celu zminimalizowania ewentualnych negatywnych skutków naruszenia;
Hasło	ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
Identyfikator	ciąg znaków literowych, cyfrowych lub innych znaków identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
Identyfikacja ryzyka	proces powtarzalny (systematyczny) i zintegrowany z procesem planowania działalności – winien być dokonywany w sposób udokumentowany nie rzadziej niż raz w roku w odniesieniu do celów i zadań, zaś na bieżąco, jako element rutynowego działania pracowników – ryzyko może mieć swoje źródło wewnątrz jednostki jak i w środowisku w jakim jednostka funkcjonuje (przyczyny/ czynniki wewnętrzne i zewnętrzne);
Incydent	zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo informacji, ochronę danych osobowych oraz cyberbezpieczeństwo;
Incydent poważny	incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej. Za incydent poważny będzie uznany incydent, który po szacowaniu ryzyka

	zostanie określony na poziomie wysoki i bardzo wysoki, zgodnie z BI-3 – Polityką zarządzania ryzykiem;
Informacja (dana)	wszystko, co posiada logiczne znaczenie jako przekaz treści i może być praktycznie wykorzystane w procesach, skutkując osiągnięciem celu. Informacja może być przetwarzana na różnych typach nośników (m.in. papierowych, magnetycznych, optycznych itp.), w szczególności w systemach informatycznych;
Informacja objęta tajemnicą przedsiębiorstwa	nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności;
Informacja publiczna	każda informacja o sprawach publicznych odnosząca się do organu władzy publicznej i dotycząca sfery jego działalności, w tym treść dokumentów, treść wystąpień, opinii i ocen przez nie dokonywanych;
Integralność	zasada dotycząca bezpieczeństwa informacji zapewniająca, że dane nie zostały zmienione, dodane lub usunięte w nieautoryzowany sposób;
Inspektor Ochrony Danych (IOD)	osoba pełniąca funkcję inspektora ochrony danych w rozumieniu art. 37 RODO wyznaczona przez Dyrektora ICZMP;
Istotność ryzyka	iloczyn prawdopodobieństwa i wpływu ryzyka określający potencjalny skumulowany poziom wpływu ryzyka na osiąganie przez ICZMP zamierzonych celów;
Kierownik komórki organizacyjnej	pracownik zajmujący kierownicze stanowisko w ICZMP, jak również kierownika jednostki, oraz bezpośredni przełożony osoby zajmującej samodzielne stanowisko pracy;
Klient VPN	oprogramowanie niezbędne do zainstalowania i skonfigurowania na komputerze z którego będzie uzyskiwany zdalny dostęp do zasobów sieci ICZMP;
KRI	Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;
Naruszenie bezpieczeństwa informacji	przypadek, w którym użytkownik lub inna osoba pomija lub niszczy ustanowione zabezpieczenia lub środki ochrony w celu pozyskania nieuprawnionego dostępu do informacji lub do pozostałych zasobów systemu informatycznego;
Niezaprzeczalność	zdolność do udowodnienia, że wystąpiły deklarowane zdarzenia lub działania oraz że wywołał je dany podmiot; brak możliwości zanegowania swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie;
Niezgodność	niespełnienie wymagań bezpieczeństwa informacji (PN-ISO/IEC 27000);
Nośnik wymienny	płyty CD, DVD, zewnętrzne dyski twarde, dyskietki, pamięci USB, dyski magnetooptyczne;
Obsługa incydentu	czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu;
Ocena ryzyka	proces porównywania ryzyka z założonymi kryteriami ryzyka w celu wyznaczenia wagi ryzyka;
Operator usługi kluczowej (OUK)	podmiot, wobec którego Minister Zdrowia wydał decyzję o uznaniu za operatora usługi kluczowej;

Oprogramowanie obce	oprogramowanie spoza pakietu podstawowego, tj. programy, które nie zostały zatwierdzone do użytkowania przez ICZMP;
Osoba upoważniona	osoba upoważniona przez administratora do przetwarzania danych osobowych, nad którą administrator sprawuje bezpośrednią kontrolę w procesie przetwarzania danych realizowanym przez tę osobę;
OWU NASK	osoba odpowiedzialna za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, tj. CSIRT NASK, wyznaczona odrębnym Zarządzeniem Dyrektora ICZMP;
PBI	Polityka bezpieczeństwa informacji;
Pełnomocnik ds. SZBI	osoba odpowiedzialna za bezpieczeństwo informacji w ICZMP wyznaczona odrębnym Zarządzeniem Dyrektora ICZMP;
Personel ICZMPa	osoba zatrudniona przez ICZMP na podstawie umowy o pracę oraz osoba świadcząca na rzecz ICZMP usługi na podstawie innych umów cywilnoprawnych, a także praktykanci, wolontariusze, stażyści i studenci;
Plany ciągłości działania	udokumentowany zbiór procedur awaryjnych i informacji, które są opracowane, gromadzone i utrzymywane w stanie gotowym do użycia w przypadku wystąpienia incydentu, aby umożliwić ICZMP kontynuowanie wykonywanych działań krytycznych na możliwym do przyjęcia wcześniej określonym poziomie;
Plan odtworzeniowy	dokument zawierający szczegółowy opis postępowania w przypadku wystąpienia określonego zdarzenia (awarii lub katastrofy), mającego na celu usunięcie skutków lub przyczyn awarii lub katastrofy;
Podatność	właściwość systemu informacyjnego, która może być wykorzystana przez zagrożenie w szczególności cyberbezpieczeństwa;
Podmiot przetwarzający	osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarzana dane osobowe w imieniu administratora;
Podmiot zewnętrzny	wszyscy pracownicy m.in. wykonawców i kontrahentów, dostawców produktów, materiałów i usług, wykonujących czynności w imieniu i na rzecz ICZMP lub mających dostęp do aktywów ICZMP w związku z realizacją zawartej umowy lub porozumienia;
Poufność	właściwość, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom;
Praca zdalna	praca określona w umowie o pracę, umowie zlecenia, umowie o współpracy oraz innej umowie cywilnoprawnej łączącej personel ICZMP ze ICZMP, wykonywaną przez czas oznaczony poza miejscem jej stałego wykonywania, jeżeli wykonywanie pracy poza takim miejscem jest możliwe;
Prawdopodobieństwo	oczekiwana częstość materializacji danego ryzyka;
Przetwarzanie danych osobowych	operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
Przetwarzanie	jakiekolwiek operacje wykonywane na informacjach obejmujące ich

informacji	zbieranie, gromadzenie, utrwalanie, przechowywanie, opracowywanie, zmienianie, wytwarzanie, udostępnianie, przekazywanie i usuwanie;
Pseudonimizacja	przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
PUODO	niezależny organ publiczny powołany w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych w Unii Europejskiej, zgodnie z art. 51 RODO, tj. Prezes Urzędu Ochrony Danych Osobowych;
Rejestr czynności przetwarzania danych osobowych	Dokument, o którym mowa w art. 30 ust. 1 RODO, prowadzony w formie pisemnej przez administratora, udostępniany organowi nadzorczemu, tj. PUODO na jego żądanie;
Rejestr wszystkich kategorii czynności przetwarzania	Dokument, o którym mowa w art. 30 ust. 2 RODO, prowadzony w formie pisemnej przez podmiot przetwarzający, udostępniany organowi nadzorczemu, tj. PUODO na jego żądanie;
RODO	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
Rola	grupa uprawnień przypisanych do stanowiska pracy: np. administracja, lekarz, pielęgniarka, ratownik medyczny, rehabilitant, technik elektroradiolog, rozliczenia, kadry, płace, księgowość.
Rozliczalność	właściwość informacji, polegająca na tym, że określone działanie dowolnego podmiotu może być jednoznacznie przypisane temu podmiotowi; właściwość systemu pozwalająca przypisać określone działanie w systemie do osoby fizycznej lub procesu oraz umiejscowić je w czasie zgodnie z KRI;
Ryzyko	kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencje;
Ryzyko rezydualne (szczątkowe)	ryzyko pozostałe po wdrożeniu planu działań w zakresie danego ryzyka wrodzonego;
Skutek	efekt materializacji ryzyka;
System informacyjny	uporządkowany układ odpowiednich elementów, charakteryzujących się pewnymi właściwościami i połączonych wzajemnie określonymi relacjami;
System informatyczny (teleinformatyczny)	zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego;
Szacowanie ryzyka	całościowy proces identyfikacji, analizy i oceny ryzyka;
SZBI	System Zarządzania Bezpieczeństwem Informacji w ICZMP - część całościowego systemu zarządzania (struktura polityki, procedur, wytycznych i związanych z tym zasobów służących do osiągnięcia celów ICZMP) oparta na podejściu wynikającym z ryzyka, odnosząca się do

	ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji;
ICZMP	Instytut „Centrum Zdrowia Matki Polki" w Łodzi;
UKSC	ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
Usługa kluczowa	usługa, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienioną w wykazie usług kluczowych;
VPN (ang. Virtual Private Network, pol. Wirtualna Sieć Prywatna)	technologia umożliwiająca zdalny, szyfrowany dostęp do zasobów i usług sieci teleinformatycznej poprzez sieć publiczną operatora telekomunikacyjnego;
Właściciel ryzyka	osoba, która ze względu na zajmowane stanowisko i przydział odpowiedzialności zarządza głównymi czynnikami ryzyka, przypisanego do niej. Właścicielami ryzyka mogą być dyrektorzy, kierownicy, samodzielne stanowiska lub pełnomocnicy odpowiadający za zarządzane przez nich procesy przetwarzania danych osobowych;
Wnioskodawca	użytkownik lub osoba zainteresowana wprowadzeniem nowej lub zmiany istniejącej funkcjonalności w systemie informatycznym lub aplikacji;
Upoważnienie	oświadczenie nadane przez administratora wskazujące z imienia i nazwiska osobę, która ma prawo przetwarzać dane w zakresie wskazanym w tym oświadczeniu, nad którą administrator sprawuje bezpośrednią kontrolę w procesie przetwarzania danych realizowanym przez tę osobę;
Uwierzytelnianie	działanie, którego celem jest weryfikacja deklarowanej tożsamości osoby upoważnionej;
Urządzenie mobilne	urządzenie przenośne, jak komputery przenośne (notebooki, laptopy), a także urządzenia multimedialne (projektory oraz aparaty i kamery cyfrowe) i telefony komórkowe, smartfony, tablety;
Użytkownik	każdy, kto posiada uprawnienie do korzystania z systemu informatycznego i dzięki niemu uczestniczy w przetwarzaniu informacji;
Zabezpieczenie	środki służące zarządzaniu ryzykiem, łącznie z politykami, procedurami, zaleceniami, praktyką lub strukturami organizacyjnymi, które mogą mieć naturę administracyjną, techniczną, zarządczą lub prawną;
Zagrożenie	potencjalna przyczyna niepożądanego incydentu, który powoduje, że ryzyko materializuje się w postaci wymiernej straty poprzez wystawienie danych osobowych na utratę, ujawnienie, zniszczenie lub zmianę;
Zagrożenie cyberbezpieczeństwa	potencjalna przyczyna wystąpienia incydentu;
Zarządzanie incydentem	obsługa incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi incydentu;
Zarządzanie ryzykiem	skoordynowane działania w zakresie zarządzania cyberbezpieczeństwem w odniesieniu do oszacowanego ryzyka; systematyczne stosowanie zasad zarządzania, procedur i praktyk na rzecz działań w zakresie informowania, konsultowania, tworzenia kontekstu oraz identyfikowania, analizy, oceny, postępowania z ryzykiem, monitorowania i przeglądania ryzyka związanego z przetwarzaniem informacji;
Zarządzanie	całościowy proces zarządzania identyfikujący potencjalne zagrożenia i

ciągłością działania	skutki, jakie te zagrożenia mogą wywierać na działalność ICZMP w przypadku ich wystąpienia, który zapewnia kształtowanie odporności ICZMP i umożliwia skuteczną reakcję w celu ochrony interesów kluczowych interesariuszy tj. osób zaangażowanych w działalność ICZMP, reputacji i wizerunku ICZMP;
Zdarzenie związane z bezpieczeństwem informacji	stwierdzone wystąpienie stanu systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji lub błąd zabezpieczenia, lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem informacji;
Zespół ds. Bezpieczeństwa Informacji	zespół osób powołany Zarządzeniem Dyrektora ICZMP, realizujący działania oraz opracowujący dokumenty niezbędne do prawidłowego przebiegu procesu wdrożenia SZBI wg wymagań normy ISO 27001;
Zespół ds. Cyberbezpieczeństwa	zespół osób powołany Zarządzeniem Dyrektora ICZMP, realizujący zadania wskazane w art. 8 pkt. 4 i 6, art. 11 ust. 1 pkt. 1-5, art. 12 i art. 13 UKSC;
Zespół ds. Zarządzania Ciągłością Działania	wewnętrzna struktura odpowiedzialna za zarządzanie ciągłością działania w ICZMP powołana odrębnym Zarządzeniem Dyrektora ICZMP.

Załącznik nr 2 do Polityki PP/01 – SZBI – **Wykaz aktów prawnych i innych dokumentów związanych z bezpieczeństwem informacji**

1. Podstawowe akty prawa powszechnie obowiązującego związane z bezpieczeństwem informacji:

   1) Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
   2) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
   3) Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;
   4) Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
   5) Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta;
   6) Ustawa z dnia z dnia 15 kwietnia 2011 r. o działalności leczniczej;
   7) Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia;
   8) Ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych;
   9) Ustawy z dnia z 27 sierpnia 2009 r. o finansach publicznych;
   10) Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej;
   11) Ustawa z dnia 11 września 2019 r. prawo zamówień publicznych;
   12) Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy;
   13) Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach;
   14) Ustawa z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych;
   15) Ustawa z dnia 29 września 1994 roku o rachunkowości;
   16) Ustawa z dnia 6 czerwca 1997 r. Kodeks karny;
   17) Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia;
   18) Ustawa z dnia 27 lipca 2001 roku o ochronie baz danych;
   19) Ustawa z dnia 16 grudnia 2016 r. o zasadach zarządzania mieniem państwowym;
   20) Ustawa z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną;
   21) Rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny;
   22) Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych;
   23) Rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo;
   24) Rozporządzenie Rady Ministrów z dnia 16 października 2028 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej;
   25) Rozporządzenie Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu;
   26) Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;
   27) Rozporządzenie Ministra Zdrowia z dnia 8 maja 2018 r. w sprawie rodzajów elektronicznej dokumentacji medycznej;
   28) Rozporządzenie Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania.

2. Inne dokumenty powiązane z bezpieczeństwem informacji:
   1) Statut Instytutu „Centrum Zdrowia Matki Polki w Łodzi na dzień 16 stycznia 2019 r.,
   2) Regulamin organizacyjny Instytutu „Centrum Zdrowia Matki Polki" w Łodzi,
   3) Decyzja Ministra Zdrowia z dnia 19 lipca 2022 r. uznająca Instytut „Centrum Zdrowia Matki Polki" w Łodzi za operatora usługi kluczowej w sektorze ochrony zdrowia.