



Międzyleski Szpital Specjalistyczny w Warszawie

System Zarządzania Bezpieczeństwem Informacji

SZBI-01-P – Polityka Bezpieczeństwa Informacji

Wersja
2.0.

Data wydania:
2025-12-31

Strona:

1 / 36

Załącznik nr 1
do Zarządzenia nr 120/2025 Dyrektora
Międzyleskiego Szpitala Specjalistycznego w Warszawie

Polityka Bezpieczeństwa Informacji

OPRACOWAŁ	WŁAŚCICIEL PROCEDURY
Pełnomocnik ds. SZBI	Pełnomocnik ds. SZBI
Data i podpis:	Data i podpis:
SPRAWDZIŁ	ZATWIERDZIŁ
Radca Prawny	Dyrektor
Data i podpis:	Data i podpis:



Międzyleski Szpital Specjalistyczny w Warszawie

System Zarządzania Bezpieczeństwem Informacji

Wersja
2.0.

Data wydania:
2025-12-31

SZBI-01-P – Polityka Bezpieczeństwa Informacji

Strona:

2 / 36

I. DEKLARACJA NAJWYŻSZEGO KIEROWNICTWA

Zgodnie z treścią § 19 ust. 1 Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, w Międzyleskim Szpitalu Specjalistycznym w Warszawie (dalej „Szpital”), 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 Szpitalu, 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 Szpital 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 Szpitala 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 Szpitala;
3. promowanie ciągłego doskonalenia ustanowionego SZBI;
4. kierowanie i aktywne wspieranie osób przyczyniających się do osiągnięcia skuteczności SZBI oraz stałe podnoszenie świadomości personelu Szpitala w zakresie bezpieczeństwa informacji i ciągłości działania.

W tabeli, stanowiącej załącznik nr 3 do Polityki bezpieczeństwa informacji umieszczono opis przyjętych przez Szpital zabezpieczeń i uzasadnienia ich stosowania, które odnoszą się i mają zastosowanie dla aktywów informacyjnych Systemu Zarządzania Bezpieczeństwem Informacji.

	Międzyleski Szpital Specjalistyczny w Warszawie		
	System Zarządzania Bezpieczeństwem Informacji SZBI-01-P – Polityka Bezpieczeństwa Informacji	Wersja 2.0.	Data wydania: 2025-12-31
		Strona:	3 / 36

Stosowane zabezpieczenia oparte są o rezultaty i wnioski wynikające z procesów szacowania i postępowania z ryzykiem, wymagań prawnych, wymagań kontraktowych, wymagań biznesowych organizacji w odniesieniu do bezpieczeństwa informacji.

II. WPROWADZENIE

1. Niniejsza Polityka Bezpieczeństwa Informacji jest dokumentem głównym ustanowionego w Szpitalu Systemu Zarządzania Bezpieczeństwem Informacji.
2. Dokument ma charakter deklaracyjny, zawiera ogólne ramy, wymagania, zasady, procedury i instrukcje w zakresie ochrony informacji przetwarzanych w Szpitalu oraz nadrzędny w stosunku do pozostałych wewnętrznych aktów prawnych dotyczących bezpieczeństwa informacji obowiązujących w Szpitalu, 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. Deklarację stosowania stanowi załącznik nr 3 do niniejszej Polityki.
6. Polityka Bezpieczeństwa Informacji podlega przeglądom pod kątem aktualności, przydatności i adekwatności, zgodnie z zasadami monitorowania i aktualizacji dokumentacji bezpieczeństwa określonymi w Polityce monitorowania i nadzoru nad bezpieczeństwem informacji.

III. CELE BEZPIECZEŃSTWA INFORMACJI

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



Międzyleski Szpital Specjalistyczny w Warszawie

System Zarządzania Bezpieczeństwem Informacji

Wersja
2.0.


Data wydania:
2025-12-31

SZBI-01-P – Polityka Bezpieczeństwa Informacji

Strona:

4 / 36

2. Ustanowione cele bezpieczeństwa wspierają przyjętą strategię i realizację celów ustawowych oraz strategicznych Szpitala, jak i zadań wykonywanych przez personel Szpitala, współpracowników, praktykantów, stażystów, wolontariuszy oraz inne osoby i podmioty zewnętrzne wykonujące czynności w imieniu i na rzecz Szpitala lub mające dostęp do aktywów informacyjnych Szpitala.
3. Do głównych celów bezpieczeństwa informacji w Szpitalu należy:
 - a) zapewnienia bezpieczeństwa przetwarzanych danych osobowych, w szczególności:
 - dane przetwarzane w celach zdrowotnych, których przetwarzanie nie wymaga zgody pacjenta,
 - dane przetwarzane w celach innych niż zdrowotne, których przetwarzanie nie wymaga zgody pacjenta,
 - dane przetwarzane na podstawie zgody pacjenta w celach marketingowych, w związku z realizacją badań klinicznych lub innych badań naukowych, w związku ze zautomatyzowanym podejmowaniem decyzji w indywidualnych sprawach, przekazywaniem danych osobowych do państwa trzeciego, gdy realizowane jest na podstawie zgody, lub innych celach wymagających zgody pacjenta,
 - b) zapewnienie bezpieczeństwa aktywów informacyjnych Szpitala (w tym ochrona wizerunku i relacji z podmiotami zewnętrznymi) zgodnie z wymogami obowiązującego prawa oraz adekwatnie do wyników szacowania ryzyka w bezpieczeństwie informacji,
 - c) usprawnienie funkcjonowania Szpitala poprzez uporządkowanie zasad przetwarzania informacji oraz zarządzanie aktywami informacyjnymi w zorganizowany sposób, tak aby ułatwić ciągłe doskonalenie i dostosowanie do bieżących celów Szpitala,
 - d) minimalizowanie ryzyka i ograniczanie skutków utraty bezpieczeństwa informacji,
 - e) stałe podnoszenie świadomości personelu oraz pozostałych osób i podmiotów, współpracujących ze Szpitalem w zakresie bezpieczeństwa informacji.
4. W ramach realizacji ww. celów, adekwatnie do poziomu zidentyfikowanych zagrożeń podejmowane są działania w kierunku osiągnięcia poziomu organizacyjnego i technicznego Szpitala, 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.

	Międzyleski Szpital Specjalistyczny w Warszawie		
	System Zarządzania Bezpieczeństwem Informacji	Wersja 2.0.	Data wydania: 2025-12-31
	SZBI-01-P – Polityka Bezpieczeństwa Informacji	Strona:	5 / 36

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

IV. KONTEKST SZPITALA

1. Międzyleski Szpital Specjalistyczny w Warszawie jest podmiotem leczniczym niebędącym przedsiębiorcą w rozumieniu ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej.
2. Podmiotem tworzącym Szpital jest samorząd Województwa Mazowieckiego.
3. Szpital realizuje zadania samorządu województwa w zakresie promocji i ochrony zdrowia.
4. Celem działania Szpitala jest:
 - 1) wykonywanie działalności leczniczej poprzez udzielanie świadczeń zdrowotnych;
 - 2) promocja zdrowia;
 - 3) realizacja zadań dydaktycznych i badawczych w powiązaniu z udzielaniem świadczeń zdrowotnych i promocją zdrowia, w tym wdrażanie nowych technologii medycznych oraz metod leczenia.
5. Realizując cele określone powyżej, Szpital uczestniczy w:
 - 1) przygotowywaniu osób do wykonywania zawodu medycznego i kształceniu osób wykonujących zawód medyczny;
 - 2) prowadzeniu prac badawczych (badania kliniczne, eksperymenty medyczne).
6. Do podstawowych zadań Szpitala należy udzielanie ubezpieczonym oraz innym osobom uprawnionym stacjonarnych oraz ambulatoryjnych świadczeń zdrowotnych.
7. Szpital realizuje zadania na rzecz bezpieczeństwa i obronności państwa.
8. Szpital może organizować i prowadzić punkt szkolenia dla innych podmiotów leczniczych w zakresie wykonywania zawodów medycznych, organizacji pracy oddziałów szpitalnych, zarządzania w służbie zdrowia i prawa medycznego.
9. W wykonywaniu zadań Szpital współpracuje z:
 - 1) innymi podmiotami wykonującymi działalność leczniczą,



Międzyleski Szpital Specjalistyczny w Warszawie

System Zarządzania Bezpieczeństwem Informacji

Wersja
2.0.

Data wydania:
2025-12-31

SZBI-01-P – Polityka Bezpieczeństwa Informacji

Strona:

6 / 36

- 2) stacjami sanitarno-epidemiologicznymi,
 - 3) organizacjami społecznymi,
 - 4) innymi niż wykonujące działalność leczniczą podmiotami,
 - 5) osobami fizycznymi,
- w zakresie niezbędnym do realizacji celów statutowych.
10. Szpital może prowadzić wyodrębnioną organizacyjnie działalność, w tym gospodarczą, inną niż działalność leczniczą, polegająca na:
- 1) dzierżawie lub wynajmie:
 - a) nieruchomości własnych lub dzierżawionych;
 - b) pomieszczeń;
 - c) sprzętu i aparatury;
 - 2) świadczeniu usług:
 - a) parkingowych;
 - b) transportowych;
 - c) sterylizacyjnych.
11. Szpital może prowadzić szkolenia, konferencje, kursy, w zakresie szeroko rozumianej promocji zdrowia dla placówek szkolnych, oświatowych, organizacji społecznych, stowarzyszeń, zainteresowanych osób fizycznych oraz udostępniać swoje mienie na ten cel innym podmiotom, w tym udostępniać oddziały na potrzeby wykonywania zadań dydaktycznych i badawczych w powiązaniu z udzielaniem świadczeń zdrowotnych.
12. W skład Szpitala wchodzi zakłady leczenia stacjonarnego i leczenia ambulatoryjnego oraz jednostki i komórki organizacyjne.
13. Szczegółową strukturę organizacyjną Szpitala określa regulamin organizacyjny ustalany przez Dyrektora.
14. Interesariuszami Szpital są w szczególności:
- 1) pacjenci Szpitala;
 - 2) pracownicy Szpitala;
 - 3) dostawcy, kontrahenci i inne osoby oraz podmioty realizujące zadania w imieniu i na rzecz Szpitala;
 - 4) Samorząd Województwa Mazowieckiego;
 - 5) Minister Zdrowia;
 - 6) Narodowy Fundusz Zdrowia;
 - 7) Prezes Urzędu Ochrony Danych Osobowych;



Międzyleski Szpital Specjalistyczny w Warszawie

System Zarządzania Bezpieczeństwem Informacji

Wersja
2.0.

Data wydania:
2025-12-31

SZBI-01-P – Polityka Bezpieczeństwa Informacji

Strona:

7 / 36

- 8) CSIRT NASK;
 - 9) podmioty biorące udział w ogłaszanych i przeprowadzanych przez Szpital naborach wniosków na realizację projektów;
 - 10) podmioty, który zawarły umowę z Szpital na realizację i dofinansowanie projektu (beneficjenci);
 - 11) inne niż ww. organy administracji publicznej;
 - 12) media.
15. Szpital funkcjonuje oraz realizuje swoje zadania z uwzględnieniem określonych warunkowań zewnętrznych, jak i wewnętrznych.
16. W warunkowaniach 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 osiągnięcie celów strategicznych Szpitala,
 - 4) relacje i kontakty z zewnętrznymi podmiotami publicznymi i prywatnymi (w tym umowy z kontrahentami i dostawcami),
 - 5) wizerunek Szpitala.
17. W ramach warunkowań wewnętrznych, uwzględnia się w szczególności:
- 1) strukturę organizacyjną Szpitala, podział kompetencji, ustanowione role i odpowiedzialności,
 - 2) strategię, 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 Szpitala, systemy informatyczne),
 - 5) relacje wewnętrzne i komunikację w Szpitalu (m.in. przepływ informacji w formie tradycyjnej i za pośrednictwem systemu elektronicznego obiegu dokumentów),
 - 6) przyjęte normy, wytyczne i standardy.



Międzyleski Szpital Specjalistyczny w Warszawie

System Zarządzania Bezpieczeństwem Informacji

Wersja
2.0.

Data wydania:
2025-12-31

SZBI-01-P – Polityka Bezpieczeństwa Informacji

Strona:

8 / 36

18. Kontekst funkcjonowania Szpitala 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 Szpitalu 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) wypowiedane słownie,
 - d) będące własnością Szpitala 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 Szpitalu działań i zadań, w tym:
 - a) personel (wszyscy pracownicy Szpitala bez względu na podstawę zatrudnienia, praktykanci, stażyści, wolontariusze oraz inne osoby i podmioty zewnętrzne wykonujące czynności w imieniu i na rzecz Szpitala lub mające dostęp do aktywów informacyjnych Szpitala),
 - b) budynki i pomieszczenia Szpitala, 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 Szpitala).
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



Międzyleski Szpital Specjalistyczny w Warszawie

System Zarządzania Bezpieczeństwem Informacji

Wersja
2.0.

Data wydania:
2025-12-31

SZBI-01-P – Polityka Bezpieczeństwa Informacji

Strona:

9 / 36

informacji niejawnych w Szpitalu określone zostały w treści odrębnych uregulowań wewnętrznych.

VI. PODSTAWOWE ZASADY BEZPIECZEŃSTWA INFORMACJI

1. Dążąc do możliwie 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 Szpitala odbywać się może tylko w oparciu o formalne uprawnienia do korzystania z wybranych aktywów,



Międzyleski Szpital Specjalistyczny w Warszawie

System Zarządzania Bezpieczeństwem Informacji

Wersja
2.0.

Data wydania:
2025-12-31

SZBI-01-P – Polityka Bezpieczeństwa Informacji

Strona:

10 / 36

- 9) **zasada „wiedzy uzasadnionej”** – personel Szpitala 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 Szpitala oraz inne podmioty zewnętrzne wykonujące czynności w imieniu i na rzecz Szpitala lub mające dostęp do aktywów informacyjnych Szpitala są zobowiązani do przestrzegania obowiązujących w Szpitalu zasad bezpieczeństwa.

VII. ROLA I ODPOWIEDZIALNOŚĆ W ZAKRESIE BEZPIECZEŃSTWA INFORMACJI

1. Właściwe zarządzanie bezpieczeństwem informacji w Szpitalu zapewnia struktura organizacyjna, w której skład wchodzi w szczególności:
 - 1) Dyrektor Szpitala;
 - 2) Pełnomocnik ds. SZBI;
 - 3) Inspektor Ochrony Danych;
 - 4) Administrator Systemu;
 - 5) Kierownik Działu Informatyki;
 - 6) kierujący komórkami organizacyjnymi Szpitala;
 - 7) pozostały personel Szpitala.
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 Szpitala:
 - 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.



Międzyleski Szpital Specjalistyczny w Warszawie

System Zarządzania Bezpieczeństwem Informacji

Wersja
2.0.

Data wydania:
2025-12-31

SZBI-01-P – Polityka Bezpieczeństwa Informacji

Strona:

11 / 36

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 Szpitalu, 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. Administrator Systemu (ASI) odpowiada za zarządzanie systemem teleinformatycznym Szpitala. Szczegółowe obowiązki oraz uprawnienia Administratora Systemu określa Polityka użytkowania sieci teleinformatycznej.

7. Kierujący Komórkami organizacyjnymi Szpitala:

- 1) nadzorują realizację obowiązków wynikających z SZBI przez podległy im personel Szpitala;
- 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;

	Międzyleski Szpital Specjalistyczny w Warszawie		
	System Zarządzania Bezpieczeństwem Informacji	Wersja 2.0.	Data wydania: 2025-12-31
	SZBI-01-P – Polityka Bezpieczeństwa Informacji	Strona:	12 / 36

5) zarządzają ciągłością działania w podlegających im obszarach.

8. Personel Szpitala:

- 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 Informatycznego 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 Polityką zarządzania incydemem (BI-4-U).


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 Szpitala oraz proponowanie rozwiązań ograniczających ryzyko wynikające z tych zagrożeń,
- 2) analizowanie oprogramowania szkodliwego i określanie jego wpływu na system informacyjny Szpitala;
- 3) wykrywanie przetamania lub ominięcia zabezpieczeń systemu informacyjnego Szpitala, prowadzenie analizy powłamaniowej wraz z określeniem działań niezbędnych do przywrócenia sprawności systemu informacyjnego Szpitala,
- 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.

	Międzyleski Szpital Specjalistyczny w Warszawie		
	System Zarządzania Bezpieczeństwem Informacji SZBI-01-P – Polityka Bezpieczeństwa Informacji	Wersja 2.0.	Data wydania: 2025-12-31
		Strona:	13 / 36

VIII. KLASYFIKACJA INFORMACJI

1. Informacje przetwarzane w Szpitalu 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 Szpitala (informacje, których ujawnienie mogłoby narazić Szpital 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 politykach bezpieczeństwa, stanowiących załączniki do niniejszej Polityki.

IX. STRUKTURA DOKUMENTACJI SZBI

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 na w postaci zarządzeń i decyzji przez Dyrektora Szpitala.
3. Drugą z klas dokumentacji jest dokumentacja operacyjna, sporządzana w ramach prowadzenia bieżącej działalności Szpitala, 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 trójpoziomą dokumentację bezpieczeństwa określającą zasady i tryb zarządzania bezpieczeństwem informacji oraz aktywów wspierających przedmiotowe przetwarzanie w Szpitalu:
 - 1) w ramach I poziomu SZBI (dokumenty o charakterze publicznym, ogólnodostępnym) wyróżnia się Politykę Bezpieczeństwa Informacji, która:



Międzyleski Szpital Specjalistyczny w Warszawie

System Zarządzania Bezpieczeństwem Informacji

Wersja
2.0.

Data wydania:
2025-12-31

SZBI-01-P – Polityka Bezpieczeństwa Informacji

Strona:

14 / 36

- stanowi dokument nadrzędny w stosunku do pozostałych wewnętrznych aktów prawnych dotyczących bezpieczeństwa informacji obowiązujących w Szpitalu, tworzących wspólnie dokumentację bezpieczeństwa,
 - określa ogólne ramy, kierunki, zasady i wymogi bezpieczeństwa informacji w Szpitalu oraz zakres dokumentacji bezpieczeństwa na pozostałych poziomach,
 - jest wprowadzana i aktualizowana w formie zarządzenia Dyrektora Szpitala.
- 2) W ramach II poziomu SZBI (dokumenty dedykowane i udostępniane całemu personelowi Szpitala, w uzasadnionych przypadkach wybranym osobom i podmiotom zewnętrznym wykonującym czynności w imieniu i na rzecz Szpitala lub mającym dostęp do aktywów informacyjnych Szpitala) 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 incydemem,
 - 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 Dyrektora Szpitala.
- 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 Szpitala,



Międzyleski Szpital Specjalistyczny w Warszawie

System Zarządzania Bezpieczeństwem Informacji

Wersja
2.0.

Data wydania:
2025-12-31

SZBI-01-P – Polityka Bezpieczeństwa Informacji


Strona:

15 / 36

- c) wprowadzane i aktualizowane w formie załączników do dokumentów II poziomu SZBI lub dokumentów wewnętrznych wybranych komórek organizacyjnych Szpitala, ewentualnie na mocy odrębnych zarządzeń Dyrektora Szpitala,
 - 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 Szpitalu (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 uszczegółwiają wybrane kwestie zidentyfikowane w ramach dokumentacji II poziomu.
3. W przyjętym w Szpitalu 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 Polityce monitorowania i nadzoru nad bezpieczeństwem informacji.

X. KONTROLA DOSTĘPU DO INFORMACJI

1. W ramach zapewnienia ograniczonego dostępu do aktywów informacyjnych Szpitala, 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 Szpitala zostały uregulowane w Polityce bezpieczeństwa fizycznego i środowiskowego oraz dedykowanych procedurach III poziomu SZBI.

	Międzyleski Szpital Specjalistyczny w Warszawie		
	System Zarządzania Bezpieczeństwem Informacji SZBI-01-P – Polityka Bezpieczeństwa Informacji	Wersja 2.0.	Data wydania: 2025-12-31
		Strona:	16 / 36

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 Polityce 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 bezpieczeństwa informacji.

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.



Międzyleski Szpital Specjalistyczny w Warszawie

System Zarządzania Bezpieczeństwem Informacji

Wersja
2.0.

Data wydania:
2025-12-31

SZBI-01-P – Polityka Bezpieczeństwa Informacji

Strona:

17 / 36

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 Szpitala 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 Szpitala, oraz inne osoby lub podmioty wykonujące czynności w imieniu i na rzecz Szpitala lub mające dostęp do aktywów informacyjnych Szpitala są świadomi odpowiedzialności i swoich obowiązków dotyczących bezpieczeństwa informacji oraz wypełniają je w odpowiedni sposób i z uwzględnieniem interesów Szpitala, 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.



Międzyleski Szpital Specjalistyczny w Warszawie

System Zarządzania Bezpieczeństwem Informacji

Wersja
2.0.

Data wydania:
2025-12-31

SZBI-01-P – Polityka Bezpieczeństwa Informacji

Strona:

18 / 36

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 zasobów ludzkich.

XVI. ZAPEWNIENIE CIĄGŁOŚCI DZIAŁANIA

1. W Szpitalu 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 Procedurze 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 Szpitala lub mającym dostęp do aktywów Szpitala, wprowadza się zasady postępowania w przypadku współpracy związanej z dostępem do aktywów informacyjnych Szpitala 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 Szpitalu 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 Szpitalu.
1. Przedmiotowe zasady i wymogi współpracy zostały uregulowane w procedurach bezpieczeństwa w relacjach z podmiotami zewnętrznymi.



Międzyleski Szpital Specjalistyczny w Warszawie

System Zarządzania Bezpieczeństwem Informacji

Wersja
2.0.

Data wydania:
2025-12-31

SZBI-01-P – Polityka Bezpieczeństwa Informacji

Strona:

19 / 36

XVIII. ZGODNOŚĆ Z PRZEPISAMI PRAWA I ZAPISAMI UMOWNYMI

1. W celu uniknięcia naruszenia obowiązujących przepisów prawa, zobowiązań ustawowych, zapisów zawartych umów i porozumień, w Szpitalu 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 Szpitalu 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 Szpitala 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 Polityce monitorowania i nadzoru nad bezpieczeństwem informacji, oraz dedykowanych procedurach.
6. Szpital 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.



Międzyleski Szpital Specjalistyczny w Warszawie

System Zarządzania Bezpieczeństwem Informacji

Wersja
2.0.

Data wydania:
2025-12-31

SZBI-01-P – Polityka Bezpieczeństwa Informacji

Strona:

20 / 36

XIX. NARUSZENIE BEZPIECZEŃSTWA INFORMACJI I ODPOWIEDZIALNOŚĆ Z TYTUŁU NARUSZENIA

1. Podstawową konsekwencją naruszenia bezpieczeństwa informacji jest obniżenie poziomu ochrony przetwarzanych informacji i aktywów wspierających ich przetwarzanie w Szpitalu.
2. Każdy, kto posiada dostęp do informacji i aktywów wspierających ich przetwarzanie w Szpitalu (personel Szpitala, jak również podmioty zewnętrzne wykonujące czynności w imieniu i na rzecz Szpitala lub mające dostęp do aktywów informacyjnych Szpitala) ma obowiązek informowania podmioty odpowiedzialne za bezpieczeństwo przetwarzania informacji w Szpitalu 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 Szpitala do odpowiedzialności dyscyplinarnej.
4. Naruszenie postanowień niniejszej Polityki przez kontrahenta Szpitala 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 Szpitala 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 Szpitalu, osoby bądź podmioty niezwiązane z ze Szpitalem mogą zgłaszać przypadki bądź podejrzenie naruszenia bezpieczeństwa aktywów informacyjnych Szpitala na adres incydent@mssw.pl.
7. Szczegółowe zasady dot. identyfikowania, zgłaszania, reagowania i obsługi zdarzeń i incydentów związanych z bezpieczeństwem informacji zostały uregulowane w Procedurze zarządzania incydentami bezpieczeństwa informacji.



Międzyleski Szpital Specjalistyczny w Warszawie

System Zarządzania Bezpieczeństwem Informacji

Wersja
2.0.

Data wydania:
2025-12-31

SZBI-01-P – Polityka Bezpieczeństwa Informacji

Strona:

21 / 36

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. UTRZYMYWANIE, 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 Szpitalu 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 Polityce monitorowania i nadzoru nad bezpieczeństwem informacji oraz innych dedykowanych procedurach.



Międzyleski Szpital Specjalistyczny w Warszawie

System Zarządzania Bezpieczeństwem Informacji

Wersja
2.0.

Data wydania:
2025-12-31

SZBI-01-P – Polityka Bezpieczeństwa Informacji

Strona:

22 / 36

XXII. INFORMOWANIE O TREŚCI DOKUMENTACJI

1. Niniejszy dokument Polityki wraz z załącznikami mają charakter jawny i są ogólnodostępne (dokumentacja „P”).
2. Dokumenty powiązane, w tym zawierające dokumentację II poziomu SZBI udostępniane są całemu personelowi Szpitala (dokumentacja „U”), a w uzasadnionych przypadkach wybranym osobom lub podmiotom zewnętrznym wykonującym czynności w imieniu i na rzecz Szpitala (dokumentacja „Z”) lub mającym dostęp do aktywów informacyjnych Szpitala.
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. ZAŁĄCZNIKI:

1. Wykaz skrótów i definicji;
2. Wykaz aktów prawnych, polskich norm i innych dokumentów związanych z bezpieczeństwem informacji;
3. Deklaracja Stosowania.

XXIV. DOKUMENTY ZWIĄZANE:

1. SZBI-02-U - Polityka ochrony danych osobowych;
2. SZBI-03-P - Polityka ciągłości działania;
3. SZBI-04-U - Procedura nadawania upoważnień;
4. SZBI-05-U - Procedura udostępniania danych;
5. SZBI-06-U - Procedura udostępniania dokumentacji medycznej;
6. SZBI-07-U - Procedura ochrony danych pacjentów;
7. SZBI-08-U - Procedura zarządzania ryzykiem bezpieczeństwa informacji;
8. SZBI-09-Z - Procedura zarządzania podatnościami;
9. SZBI-10-U - Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji;
10. SZBI-11-U - Procedura użytkowania sieci teleinformatycznej;
11. SZBI-12-U - Procedura rejestracji i inwentaryzacji oprogramowania i sprzętu komputerowego;
12. SZBI-13-U - Procedura pracy zdalnej;



Międzyleski Szpital Specjalistyczny w Warszawie

System Zarządzania Bezpieczeństwem Informacji

Wersja
2.0.


Data wydania:
2025-12-31

SZBI-01-P – Polityka Bezpieczeństwa Informacji

Strona:

23 / 36

13. SZBI-14-U - Procedura dostępu VPN do zasobów sieci;
14. SZBI-15-Z - Procedura przechowywania i przekazywania hasła administratora systemu;
15. SZBI-16-Z - Procedura wykonywania kopii zapasowych;
16. SZBI-17-U - Procedura rejestracji i inwentaryzacji sprzętu medycznego;
17. SZBI-18-U - Procedura zarządzania zmianą IT;
18. SZBI-19-U – Procedura ochrony danych w fazie projektowania oraz domyślna ochrona danych;
19. SZBI-20-U - Procedura zarządzania aktywami informacyjnymi;
20. SZBI-21-U - Procedura zarządzania bezpieczeństwem zasobów ludzkich;
21. SZBI-22-U - Procedura bezpieczeństwa fizycznego i środowiskowego;
22. SZBI-23-U - Procedura zarządzania kluczami;
23. SZBI-24-U - Procedura zarządzania uprawnieniami w systemie kontroli dostępu;
24. SZBI-25-U - Procedura dostępu do serwerowni;
25. SZBI-26-U - Procedura zarządzania systemem monitoringu wizyjnego;
26. SZBI-27-U - Procedura korzystania z bezprzewodowej sieci dla pracownika;
27. SZBI-28-U - Procedura korzystania z bezprzewodowej sieci dla gości;
28. SZBI-29-U - Procedura bezpieczeństwa w relacjach z podmiotami zewnętrznymi dla pracowników;
29. SZBI-30-P - Procedura bezpieczeństwa w relacjach z podmiotami zewnętrznymi dla dostawców;
30. SZBI-31-U - Procedura powierzenia przetwarzania danych;
31. SZBI-32-U - Procedura monitorowania i nadzoru nad bezpieczeństwem informacji;
32. SZBI-33-U - Procedura ciągłości działania;
33. SZBI-34-Z - Procedura ciągłości działania sieci teleinformatycznej;
34. SZBI-35-U - Procedura oceny skutków;
35. SZBI-36-U - Procedura audytów wewnętrznych SZBI.

	Międzyleski Szpital Specjalistyczny w Warszawie		
	System Zarządzania Bezpieczeństwem Informacji SZBI-01-P – Polityka Bezpieczeństwa Informacji	Wersja 2.0.	Data wydania: 2025-12-31
		Strona:	24 / 36

Załącznik nr 1 – 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 Szpital;
Administrator Systemu	pracownik Szpitala zarządzający prawami dostępu do systemów oraz usług w sieci teleinformatycznej Szpitala;
Aktywa	wszystko, co ma wartość dla Szpitala, a w szczególności: personel, wizerunek, informacje wytwarzane, przetwarzane i przechowywane w Szpitalu, mienie wykorzystywane przez Szpital 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 Szpitala i wymagające właściwej ochrony przed utratą dostępności, poufności i integralności;
Analiza ryzyka	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



Międzyleski Szpital Specjalistyczny w Warszawie

System Zarządzania Bezpieczeństwem Informacji

Wersja
2.0.

Data wydania:
2025-12-31

SZBI-01-P – Polityka Bezpieczeństwa Informacji

Strona:

25 / 36

	zawartość danych opisujących obiekt są takie jak deklarowane (KRI);
Badanie kliniczne	każde badanie prowadzone z udziałem ludzi w celu odkrycia lub potwierdzenia klinicznych, farmakologicznych, w tym farmakodynamicznych skutków działania jednego lub wielu badanych produktów leczniczych, lub w celu zidentyfikowania działań niepożądanych jednego lub większej liczby badanych produktów leczniczych, lub śledzenia wchłaniania, dystrybucji, metabolizmu i wydalania jednego lub większej liczby badanych produktów leczniczych, mając na względzie ich bezpieczeństwo i skuteczność, a także zaprojektowane i zaplanowane systematyczne badanie prowadzone na ludziach, podjęte w celu weryfikacji bezpieczeństwa lub działania określonego wyrobu medycznego, wyposażenia wyrobu medycznego albo aktywnego wyrobu medycznego do implantacji;
Badanie naukowe	badanie naukowe, o którym mowa w motywie 159 RODO, pojęcie to obejmuje również eksperyment medyczny, w tym badanie kliniczne;
Bezpieczeństwo informacji	zachowanie poufności, integralności i dostępności informacji; dodatkowo, mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;
Zespół ds. Reagowania na Incydenty (ZRI)	wewnętrzna struktura odpowiedzialna za cyberbezpieczeństwo w Szpitalu powołana odrębnym Zarządzeniem Dyrektora Szpitala;
Ciągłość działania	zdolność Szpitala 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;



Międzyleski Szpital Specjalistyczny w Warszawie

System Zarządzania Bezpieczeństwem Informacji

Wersja
2.0.

Data wydania:
2025-12-31

SZBI-01-P – Polityka Bezpieczeństwa Informacji

Strona:

26 / 36

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 Szpitalu;
Dokumentacja medyczna	dokumentacja medyczna, o której mowa w przepisach ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta oraz wydanych na jej podstawie aktach wykonawczych, a także określona w przepisach odrębnych;
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;
Działania zaradcze	środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym środki w celu zminimalizowania ewentualnych negatywnych skutków naruszenia;
Eksperyment medyczny	eksperyment medyczny w rozumieniu ustawy o zawodach lekarza i lekarza denty, obejmujący eksperyment leczniczy i badawczy. Pojęcie to obejmuje również badania kliniczne;
Hasło	ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;



Międzyleski Szpital Specjalistyczny w Warszawie

System Zarządzania Bezpieczeństwem Informacji

Wersja
2.0.

Data wydania:
2025-12-31

SZBI-01-P – Polityka Bezpieczeństwa Informacji

Strona:

27 / 36

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. Za incydent poważny będzie uznany incydent, który po szacowaniu ryzyka zostanie określony na poziomie wysoki i bardzo wysoki;
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 Szpitala;



Międzyleski Szpital Specjalistyczny w Warszawie

System Zarządzania Bezpieczeństwem Informacji

Wersja
2.0.

Data wydania:
2025-12-31

SZBI-01-P – Polityka Bezpieczeństwa Informacji

Strona:

28 / 36

Istotność ryzyka	ilożyczn prawdopodobieństwa i wpływu ryzyka określający potencjalny skumulowany poziom wpływu ryzyka na osiągnięcie przez Szpital zamierzonych celów;
Kierownik komórki organizacyjnej	pracownik zajmujący kierownicze stanowisko w Szpitalu, jak również kierownik 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 Szpitala;
KRI	Rozporządzenie Rady Ministrów z dnia 21 maja 2024 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 27001);
Nośnik wymienny	płyty CD, DVD, zewnętrzne dyski twarde, dyskietki, pamięci USB, dyski magnetoptyczne;
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;
Opiekun faktyczny	opiekun faktyczny w rozumieniu ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta;
Oprogramowanie obce	oprogramowanie spoza pakietu podstawowego, tj. programy, które nie zostały zatwierdzone do użytkowania przez Szpital;



Międzyleski Szpital Specjalistyczny w Warszawie

System Zarządzania Bezpieczeństwem Informacji

Wersja
2.0.

Data wydania:
2025-12-31

SZBI-01-P – Polityka Bezpieczeństwa Informacji

Strona:

29 / 36

Osoba bliska	małżonek, krewny lub powinowaty do drugiego stopnia w linii prostej, Przedstawiciel ustawowy, osoba pozostająca we wspólnym pożyciu lub osoba wskazana przez Pacjenta;
Osoba upoważniona	osoba upoważniona przez administratora do przetwarzania danych osobowych, nad którą administrator sprawuje bezpośrednią kontrolę w procesie przetwarzania danych realizowanym przez tę osobę;
Osoba wykonująca zawód medyczny	osoba uprawniona na podstawie odrębnych przepisów do udzielania świadczeń zdrowotnych oraz osoba legitymująca się nabyciem fachowych kwalifikacji do udzielania świadczeń zdrowotnych w określonym zakresie lub w określonej dziedzinie medycyny, w tym m.in. lekarz, lekarz dentysta, pielęgniarka, położna, ratownik medyczny, diagnosta laboratoryjny, fizjoterapeuta, technik analityki medycznej, farmaceuta, technik farmacji, psycholog, psychoterapeuta, logopeda, felczer, optometrysta, dietetyk, a także osoby wykonujące inne zawody wskazane w przepisach wykonawczych wydanych na podstawie art. 190 ust. 1 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych. W przypadku, gdy w SZBI mowa o pielęgniarce lub lekarzu, rozumie się przez to również odpowiednio położną i lekarza dentystę;
OWU NASK	osoba odpowiedzialna za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, tj. CSIRT NASK, wyznaczona odrębnym Zarządzeniem Dyrektora Szpitala;
Pacjent	osoba zwracającą się o udzielenie świadczeń zdrowotnych lub korzystającą ze świadczeń zdrowotnych udzielanych przez podmiot udzielający świadczeń zdrowotnych lub osobę wykonującą zawód medyczny;
Pełnomocnik ds. SZBI	osoba odpowiedzialna za bezpieczeństwo informacji w Szpitalu wyznaczona odrębnym Zarządzeniem Dyrektora Szpitala;
Personel Szpitala	osoba zatrudniona przez Szpital na podstawie umowy o pracę oraz osoba świadcząca na rzecz Szpitalu usługi na podstawie innych umów cywilnoprawnych oraz praktykanci, stażyści i wolontariusze;
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



Międzyleski Szpital Specjalistyczny w Warszawie

System Zarządzania Bezpieczeństwem Informacji

Wersja
2.0.

Data wydania:
2025-12-31

SZBI-01-P – Polityka Bezpieczeństwa Informacji

Strona:

30 / 36

	Szpitalowi 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 przetwarza 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 Szpitala lub mających dostęp do aktywów Szpitala 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 Szpitala ze Szpitalem, wykonywaną przez czas oznaczony poza miejscem jej stałego wykonywania, jeżeli wykonywanie pracy poza takim miejscem jest możliwe;
Prawdopodobieństwo	oczekiwana częstość materializacji danego ryzyka;
Profilaktyka zdrowotna	wszelkie działania mające na celu zapobieganie niekorzystnym zjawiskom w obszarze zdrowia pacjenta;
Przedstawiciel ustawowy	osoba umocowana do działania w cudzym imieniu na podstawie ustawy zgodnie z art. 96 Kodeksu cywilnego;
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,



Międzyleski Szpital Specjalistyczny w Warszawie

System Zarządzania Bezpieczeństwem Informacji

Wersja
2.0.

Data wydania:
2025-12-31

SZBI-01-P – Polityka Bezpieczeństwa Informacji

Strona:

31 / 36

	dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
Przetwarzanie informacji	jakikolwiek operacje wykonywane na informacjach obejmujące ich 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 c, prowadzony w formie pisemnej przez administratora, udostępniany organowi nadzorcemu, 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 nadzorcemu, 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



Międzyleski Szpital Specjalistyczny w Warszawie

System Zarządzania Bezpieczeństwem Informacji

Wersja
2.0.

Data wydania:
2025-12-31

SZBI-01-P – Polityka Bezpieczeństwa Informacji

Strona:

32 / 36

	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 Szpitalu - część całościowego systemu zarządzania (struktura polityki, procedur, wytycznych i związanych z tym zasobów służących do osiągnięcia celów Szpitala) oparta na podejściu wynikającym z ryzyka, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji;
Świadczenie zdrowotne	działania służące zachowaniu, ratowaniu, przywracaniu lub poprawie zdrowia oraz inne działania medyczne wynikające z procesu leczenia lub przepisów odrębnych regulujących zasady ich wykonywania
UKSC	ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
UODO	Urząd Ochrony Danych Osobowych;
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,



Międzyleski Szpital Specjalistyczny w Warszawie

System Zarządzania Bezpieczeństwem Informacji

Wersja
2.0.

Data wydania:
2025-12-31

SZBI-01-P – Polityka Bezpieczeństwa Informacji

Strona:

33 / 36

	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 incydemem	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,



Międzyleski Szpital Specjalistyczny w Warszawie

System Zarządzania Bezpieczeństwem Informacji

Wersja
2.0.


Data wydania:
2025-12-31

SZBI-01-P – Polityka Bezpieczeństwa Informacji

Strona:

34 / 36


	tworzenia kontekstu oraz identyfikowania, analizy, oceny, postępowania z ryzykiem, monitorowania i przeglądania ryzyka związanego z przetwarzaniem informacji;
Zarządzanie ciągłością działania	całościowy proces zarządzania identyfikujący potencjalne zagrożenia i skutki, jakie te zagrożenia mogą wywierać na działalność Szpitala w przypadku ich wystąpienia, który zapewnia kształtowanie odporności Szpitala i umożliwia skuteczną reakcję w celu ochrony interesów kluczowych interesariuszy tj. osób zaangażowanych w działalność Szpitala, reputacji i wizerunku Szpitala;
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. Cyberbezpieczeństwa	zespół osób powołany Zarządzeniem Dyrektora Szpitala, 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 Szpitalu powołana odrębnym Zarządzeniem Dyrektora Szpitala.

	Międzyleski Szpital Specjalistyczny w Warszawie		
	System Zarządzania Bezpieczeństwem Informacji SZBI-01-P – Polityka Bezpieczeństwa Informacji	Wersja 2.0.	Data wydania: 2025-12-31
		Strona:	35 / 36

Załącznik nr 2 – 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;

	Międzyleski Szpital Specjalistyczny w Warszawie		
	System Zarządzania Bezpieczeństwem Informacji	Wersja 2.0.	Data wydania: 2025-12-31
SZBI-01-P – Polityka Bezpieczeństwa Informacji	Strona:	36 / 36	

- 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 Międzyleskiego Szpitala Specjalistycznego w Warszawie stanowiący załącznik do uchwały nr 137/17 Sejmiku Województwa Mazowieckiego z dnia 29 sierpnia 2017 r.,
- 2) Regulamin organizacyjny podmiotu leczniczego „Międzyleski Szpital Specjalistyczny w Warszawie” stanowiący załącznik nr 2 do zarządzenia Dyrektora nr 58/2021 z dnia 29.09.2021 r. (ze zmianami).