

POLITYKA BEZPIECZEŃSTWA INFORMACJI I CYBERBEZPIECZEŃSTWA SZPITALA SPECJALISTYCZNEGO im. JĘDRZEJA ŚNIADECKIEGO w NOWYM SĄCZU

§ 1

Cel i zakres stosowania

1. **Polityka Bezpieczeństwa Informacji i Cyberbezpieczeństwa (dalej: PBliC)**, zawiera zasady dotyczące ochrony danych przetwarzanych w Szpitalu Specjalistycznym im. Jędrzeja Śniadeckiego w Nowym Sączu (dalej: Szpital). Politykę stosuje się do wszystkich przetwarzanych w Szpitalu danych; bez względu na miejsce, formę czy sposób przetwarzania, dla których Szpital jest administratorem oraz do danych współadministrowanych i powierzonych do przetwarzania.
2. Stosowanie zasad określonych w **PBliC** ma na celu:
 - a) zapewnienie prawidłowej ochrony przetwarzanych danych (także w systemach informatycznych), przed ich nieuprawnionym udostępnieniem, utratą, uszkodzeniem lub zniszczeniem;
 - b) zapewnienie:
 - poufności (informacja jest dostępna wyłącznie osobom upoważnionym),
 - integralności (zapewnienie dokładności i kompletności informacji oraz metod przetwarzania),
 - dostępności (upoważnione osoby mają dostęp do informacji i systemów),
 - rozliczalności przetwarzanych informacji (wszystkie działania związane z przetwarzaniem w systemach informatycznych umożliwiają przypisanie tych działań użytkownikowi);
 - c) wdrażanie mechanizmów cyberbezpieczeństwa.
3. Przedmiotem **PBliC** są zasady postępowania mające na celu zapewnienie bezpieczeństwa informacji oraz cyberbezpieczeństwa.
4. **PBliC** reguluje najistotniejsze zasady:
 - a) przetwarzania danych osobowych w Szpitalu;
 - b) przydzielania uprawnień do systemów informatycznych;
 - c) zgłaszania zdarzeń i incydentów cyberbezpieczeństwa.
5. **PBliC** obowiązuje wszystkie osoby przetwarzające dane osobowe.
6. **PBliC** została opracowana na podstawie aktów prawnych, m.in.:
 - Rozporządzenia 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 (Dz. U. UE. L. 2016/119/1 z późn. zm.)- dalej: RODO;
 - Ustawy z dnia 10.05.2018 r. o ochronie danych osobowych (t. j. Dz. U. z 2019 r., poz. 1781 z późn. zm.);
 - Ustawy z dnia 15.04.2011 r. o działalności leczniczej (t. j. Dz. U. z 2025 r., poz. 450 z późn. zm.);
 - Ustawy z 06.11.2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (t. j. Dz. U. z 2024 r., poz. 581 z późn. zm.);
 - Ustawy z dnia 28.04.2011 r. o systemie informacji w ochronie zdrowia (t.j. Dz. U. z 2025 r., poz. 302 z późn. zm.);

- Ustawy z dnia 26.06.1974 r. Kodeks Pracy (t. j. Dz. U. z 2025 r., poz. 277 z późn. zm.);
- Rozporządzenia Ministra Zdrowia z dnia 6.04.2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (t. j. Dz. U. z 2024 r., poz. 798);
- Ustawa o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r. (t. j. Dz. U. z 2024 r. poz. 1077, z późn. zm.);
- Rozporządzenia Rady Ministrów z dnia 21.05.2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2024 poz. 773, z późn. zm.).

Zasady ochrony informacji niejawnych reguluje ustawa o ochronie informacji niejawnych oraz opracowane na jej podstawie inne wewnętrzne regulacje Szpitala.

§ 2

Definicje i terminologia

1. **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;
2. **Przetwarzanie**- operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie 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;
3. **Administrator Danych /AD/-** Szpital Specjalistyczny im. J. Śniadeckiego w Nowym Sączu reprezentowany przez Dyrektora;
4. **Podmiot przetwarzający**- osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
5. **Odbiorca**- osoba fizyczna lub prawna; organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe;
6. **Zgoda**- dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
7. **Naruszenie ochrony danych osobowych**- naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
8. **Dane dotyczące zdrowia**- dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej- w tym o korzystaniu z usług opieki zdrowotnej- ujawniające informacje o stanie jej zdrowia;

- 9. Organ nadzorczy-** Urząd Ochrony Danych Osobowych (UODO);
- 10. Inspektor Ochrony Danych /IOD/-** osoba wyznaczona przez administratora odpowiedzialna za nadzorowanie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych;
- 11. Administrator Systemów Informatycznych /ASI/, Lokalny Administrator Systemu /LAS/-** osoba wyznaczona przez AD odpowiedzialna za funkcjonowanie systemu informatycznego, zarządzająca uprawnieniami użytkowników do tego systemu;
- 12. Osoba upoważniona-** osoba posiadająca pisemne upoważnienie AD do przetwarzania danych osobowych;
- 13. Użytkownik systemów informatycznych-** osoba, która korzysta z systemu komputerowego lub oprogramowania w celu wykonywania określonych zadań;
- 14. Cyberbezpieczeństwo-** odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych w systemach lub związanych z nimi usług;

§ 3

Odpowiedzialność i uprawnienia

Administrator Danych przydziela role i obowiązki w zakresie bezpieczeństwa danych i cyberbezpieczeństwa, tak aby nie pozostawały one w konflikcie ze sobą. Za bezpieczeństwo danych osobowych i cyberbezpieczeństwo w Szpitalu odpowiadają:

- 1. Zespół ds. cyberbezpieczeństwa-** osoby wskazane przez AD, realizujące zadania przypisane Operatorowi Usługi Kluczowej (dalej: OUK), m. in.:
 - monitorowanie zagrożeń cyberbezpieczeństwa i incydentów,
 - reagowanie na zgłoszone incydenty,
 - klasyfikowanie incydentów oraz koordynowanie obsługi incydentów krytycznych,
 - prowadzenie analizy złośliwego oprogramowania oraz analizy podatności,
 - prowadzenie działań z zakresu budowania świadomości pracowników w obszarze cyberbezpieczeństwa;
- 2. Osoba wyznaczona do kontaktu z organami nadzorczymi (np. UODO, CSIRT NASK)-** osoba wskazana przez AD, odpowiedzialna za utrzymanie kontaktów z zakresie ochrony danych i cyberbezpieczeństwa;
- 3. Inspektor Ochrony Danych /IOD/-** nadzór w zakresie zapewnienia przestrzegania przepisów o ochronie danych osobowych zgodnie z RODO, m. in.:
 - informowanie i doradztwo w zakresie obowiązków spoczywających na AD,
 - prowadzenie rejestru czynności przetwarzania danych osobowych,
 - prowadzenie analizy ryzyka dla zbiorów i czynności związanych z danymi osobowymi,
 - monitorowanie przestrzegania wymagań RODO przez pracowników,
 - opracowanie i aktualizacja wewnętrznych procedur w zakresie przetwarzania danych osobowych,
 - zapewnienie szkoleń personelu uczestniczącego w przetwarzaniu danych osobowych,
 - analiza incydentów bezpieczeństwa i podejmowanie wraz z zespołem ds. cyberbezpieczeństwa odpowiednich działań naprawczych,
 - prowadzenie audytów bezpieczeństwa danych osobowych;
- 4. Administrator Systemu Informatycznego-** odpowiedzialność za zarządzanie i bezpieczeństwo teleinformatyczne, identyfikacja podatności na zagrożenia bezpieczeństwa

Załącznik nr 1 do Zarządzenia nr 79 z dnia 16.06.2025 r.
POLITYKA BEZPIECZEŃSTWA INFORMACJI I CYBERBEZPIECZEŃSTWA
SZPITALA SPECJALISTYCZNEGO im. JĘDRZEJA ŚNIADECKIEGO
w NOWYM SĄCZU

teleinformatycznego oraz bezpieczne zarządzanie zasobami w administrowanych systemach; współpraca z IOD w zakresie niezbędnym do prawidłowej realizacji obowiązków związanych z ochroną danych osobowych;

5. Lokalny Administrator Systemu /LAS/- uprawnienia do zarządzania użytkownikami oraz danymi tego podmiotu w obrębie danego systemu, nadawanie i odbieranie uprawnień dostępowych do danych oraz wsparcie techniczne i organizacyjne w zakresie funkcjonowania systemu na poziomie lokalnym, współpraca z IOD w zakresie niezbędnym do prawidłowej realizacji obowiązków związanych z ochroną danych osobowych;

6. Zespół ds. informatycznych- zarządzanie zasobami teleinformatycznymi, w szczególności:

- wsparcie użytkowników w bieżących pracach,
- zarządzanie zasobami teleinformatycznymi w sposób zapewniający zachowanie dostępności, integralności, poufności i rozliczalności,
- zarządzanie kontrolą dostępu do zarządzanych zasobów teleinformatycznych,
- nadzór nad dostawcami/ serwisantami systemów informatycznych,
- obsługa (wraz z zespołem ds. cyberbezpieczeństwa) incydentów bezpieczeństwa teleinformatycznego,
- współpraca z IOD w zakresie niezbędnym do prawidłowej realizacji obowiązków związanych z ochroną danych osobowych;

7. Kierownik komórki organizacyjnej- zapewnienie i nadzorowanie spełnienia obowiązujących wymagań bezpieczeństwa danych osobowych i bezpieczeństwa teleinformatycznego przez podległy personel, w szczególności:

- zapewnienie prawidłowej ochrony danych i zasobów teleinformatycznych w podległej komórce organizacyjnej,
- zapewnienie, aby wszyscy pracownicy danej komórki organizacyjnej, zapoznali się z obowiązującymi procedurami w zakresie ochrony danych i złożyli oświadczenie o zapoznaniu się z nimi,
- zgłaszanie incydentów bezpieczeństwa teleinformatycznego oraz współpraca z Zespołem ds. cyberbezpieczeństwa,
- wnioskowanie do AD o nadanie/ zmianę/ odebranie uprawnień dla podległych pracowników w systemach informatycznych,
- współpraca z IOD i ASI w ramach realizowanych przez nich zadań;

8. Koordynator Działu Zatrudnienia i Płac/ Koordynator Działu Organizacji i Nadzoru - zgłaszanie do IOD i ASI wszelkich zmian związanych z zatrudnieniem, zmianą miejsca pracy i zakończeniem pracy, istotnych z uwagi na poziom dostępu do danych i systemów informatycznych;

9. Osoby upoważnione/ użytkownicy systemów informatycznych- wszystkie osoby przetwarzające dane osobowe, odpowiadające za przestrzeganie wewnętrznych procedur w zakresie ochrony danych w tym przetwarzanych w systemach teleinformatycznych, w szczególności poprzez:

- stosowanie się do wewnętrznych procedur,
- właściwe korzystanie z zasobów teleinformatycznych, z zachowaniem ostrożności, z należytą starannością oraz zgodnie z posiadanymi uprawnieniami,
- informowanie Zespołu ds. informatycznych o wszystkich zdarzeniach mających wpływ na bezpieczeństwo informacji,
- niezwłoczne zgłaszanie podejrzeń naruszeń zasad (incydentów) bezpieczeństwa teleinformatycznego IOD/ ASI/LAS/Zespołowi ds. informatycznych,
- współpraca z IOD i ASI w ramach realizowanych przez nich zadań,

- podnoszenie poziomu wiedzy z zakresu bezpieczeństwa informacji, udział w szkoleniach z zakresu ochrony danych, bezpieczeństwa informacji i cyberbezpieczeństwa.

Za utrzymanie ciągłości świadczenia usług kluczowych i cyberbezpieczeństwo, odpowiada każdy pracownik Szpitala odpowiednio do rodzaju świadczonej pracy oraz powołany Zespół odpowiedzialny za cyberbezpieczeństwo.

§ 4

Ogólne zasady dotyczące przetwarzania danych osobowych

1. Dane osobowe w Szpitalu przetwarza się zgodnie z prawem i rzetelnie.
2. Każda osoba, której dane mają być przetwarzane, jest informowana o swoich prawach i celach przetwarzania. Informacje te są przekazywane w sposób zrozumiały dla osoby informowanej.
3. Zbierane dane, muszą być ograniczone tylko do danych niezbędnych do realizacji danego celu.
4. Każdorazowo przed podaniem danych, osoba, której dane dotyczą jest informowana o miejscu, gdzie znajduje się klauzula informacyjna.
5. Klauzule informacyjne umieszcza się na tablicach informacyjnych przy rejestracjach, w oddziałach, na stronie internetowej Szpitala; są również dostępne u IOD.
6. Kierownik komórki organizacyjnej zapewnia odpowiednie zabezpieczenie informacji, tak aby żadne istotne informacje (np. dane osobowe, dane finansowe, dane dot. pacjentów nie znajdowały się w miejscach ogólnodostępnych- na tablicach ogłoszeń.
7. W przypadku przetwarzania danych, na które wymagana jest zgoda osoby, której dane dotyczą jest ona umieszczana w dokumentach dotyczących danego przetwarzania (postępowania).
8. Dane zebrane w konkretnych, wyraźnych i prawnie uzasadnionych celach, nie mogą być przetwarzane dalej w sposób niezgodny z tymi celami.
9. Przetwarzanie do celów archiwalnych, badań naukowych i statystycznych nie jest uznawane za niezgodne z pierwotnymi celami.
10. Sposób ochrony poszczególnych zbiorów zawarto w Rejestrze czynności przetwarzania danych osobowych.
11. W przypadku tworzenia nowego zbioru czy wprowadzania nowego systemu, każdorazowo przed ich wprowadzeniem IOD dokonuje analizy ryzyka (jeśli dotyczy to także DPIA- ang. *Data Protection Impact Assessment* tj. ocena skutków dla ochrony danych, przeprowadzana, aby określić czy planowane przetwarzanie danych osobowych może prowadzić do wysokiego ryzyka naruszenia praw lub wolności osób, których dane dotyczą).
12. Wszystkie dane osobowe (w szczególności dotyczące stanu zdrowia), przekazywane w sieci (np. e-mail), muszą być szyfrowane lub zabezpieczone kodem. Dotyczy to także wiadomości przesyłanych służbowo w postaci e-mail pomiędzy pracownikami Szpitala.
13. Osoby przetwarzające dane są zobowiązane dołożyć starań, aby zebrane dane osobowe były odpowiednie do zebranych celów oraz przechowywane przez okres określony w przepisach prawa.
14. Dane zbędne są usuwane.
15. Za bezpieczeństwo przetwarzanych danych osobowych w poszczególnych komórkach organizacyjnych Szpitala odpowiada każdy pracownik; który przetwarza dane osobowe; który zobowiązany jest chronić dane przed niedozwolonym lub niezgodnym z prawem przetwarzaniem, przypadkową utratą, zniszczeniem lub uszkodzeniem; głównie za pomocą określonych przez AD środków technicznych i organizacyjnych.
16. Szpital w ramach zapewnienia właściwego poziomu ochrony danych osobowych i cyberbezpieczeństwa wyznacza osoby odpowiedzialne za współpracę z organami nadzorczymi (m.in. Urząd Ochrony Danych Osobowych, CSIRT NASK).

17. Klasyfikację i zasady postępowania z informacjami przetwarzanymi w Szpitalu, zawiera

Załącznik nr 1 do PBLiC.

18. W Jednolitym Rzeczowym Wykazie Akt Szpitala zawarto spis klas pierwszego i drugiego rzędu; z podziałem na symbole kwalifikacyjne, hasła kwalifikacyjne oraz oznaczenie kategorii archiwalnej.

19. Okres archiwizacji dokumentów zawierających dane osobowe określa Instrukcja Archiwalna Szpitala.

II. Przetwarzanie szczególnych kategorii danych osobowych

1. Dane dotyczące zdrowia mogą być przetwarzane z zachowaniem możliwie najwyższych środków ich ochrony.

2. Przetwarzanie danych genetycznych odbywa się zgodnie z procedurami określonymi w Medycznym Laboratorium Diagnostycznym. Osoba której dane dotyczą jest o tym informowana i na ich przetwarzanie musi wyrazić zgodę.

3. W przypadku przetwarzania danych biometrycznych, osoba której dane dotyczą jest o tym informowana i na ich przetwarzanie musi wyrazić zgodę.

4. Nie jest wymagana zgoda do celów profilaktyki zdrowotnej lub medycyny pracy.

5. Przetwarzanie szczególnych kategorii danych osobowych, m. in.: w celach marketingowych badaniach klinicznych lub naukowych, wymaga zgody pacjenta.

III. Prawa osoby, której dane dotyczą

1. Przejrzyste informowanie i przejrzysta komunikacja oraz tryb wykonywania praw przez osobę, której dane dotyczą

1) Wszelkie informacje dotyczące przetwarzania danych osobowych należy przekazywać w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie.

2. Informacje i dostęp do danych osobowych

a) Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą

1) Rejestracja pacjenta jest dokonywana w oparciu o dowód osobisty lub inny dokument tożsamości.

2) Przed zebraniem danych osobowych, osoba zbierająca te dane, informuje, gdzie można zapoznać się z klauzulą informacyjną.

b) Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą

1) Jeżeli dane osobowe, zbierane są nie od osoby której dotyczą (np. gdy pacjent jest nieprzytomny), to niezwłocznie po odzyskaniu przytomności (świadomości) należy jej wskazać miejsce gdzie znajduje się klauzula informacyjna, a także poinformować o źródle pochodzenia danych osobowych.

3. Prawo dostępu przysługujące osobie, której dane dotyczą

1) Osoba, której dane dotyczą, ma prawo dostępu do swoich danych oraz do otrzymania kopii swoich danych.

4. Prawo do sprostowania danych

1) Osoba, której dane dotyczą, ma prawo żądania sprostowania dotyczących jej danych oraz ma prawo żądania uzupełnienia niekompletnych danych osobowych; poprzez przedstawienie dodatkowego dokumentu czy oświadczenia.

2) Pacjent ma prawo zażądać niezwłocznego sprostowania lub uzupełnienia danych zawartych w dokumentacji medycznej wyłącznie w zakresie w jakim nie będzie prowadzić to do naruszenia

autonomii zawodowej osoby wykonującej zawód medyczny, która dokonywała wpisu do dokumentacji medycznej.

5. Prawo do usunięcia danych („prawo do bycia zapomnianym”)

1) Prawo do usunięcia danych (do bycia zapomnianym) nie znajduje zastosowania wobec danych osobowych przez cały okres wymagany przepisami prawa, w tym archiwizacji dokumentacji.

6. Prawo do ograniczenia przetwarzania

1) Osoba, której dane dotyczą, może żądać od administratora oznaczenia przechowywanych danych w taki sposób, aby ograniczyć ich dalsze przetwarzanie, czyli zawęzić operacje na tych danych jedynie do ich przechowywania, w sytuacji:

- a) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych- na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;
- b) przetwarzanie jest niezgodne z prawem;
- c) AD nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
- d) osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania - do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

2) Metody pozwalające ograniczyć przetwarzanie danych osobowych to m.in.: czasowe przeniesienie wybranych danych osobowych do innego systemu przetwarzania, uniemożliwienie użytkownikom dostępu do wybranych danych, lub czasowe usunięcie opublikowanych danych ze strony internetowej. W zautomatyzowanych zbiorach danych przetwarzanie należy zasadniczo ograniczyć środkami technicznymi w taki sposób, by dane osobowe nie podlegały dalszemu przetwarzaniu ani nie mogły być zmieniane. Fakt ograniczenia przetwarzania danych osobowych należy wyraźnie zaznaczyć w systemie.

4) Przed uchycieniem ograniczenia przetwarzania administrator informuje o tym osobę, która żądała ograniczenia.

7. Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania

1) AD informuje o sprostowaniu, usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał, każdego odbiorcę, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

8. Prawo do przenoszenia danych

1) Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, jeżeli przetwarzanie odbywa się:

- a) na podstawie zgody,
- b) na podstawie umowy,
- c) w sposób zautomatyzowany.

9. Prawo do sprzeciwu oraz zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach

1) Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw- z przyczyn związanych z jej szczególną sytuacją - wobec przetwarzania dotyczących jej danych osobowych w tym profilowania.

2) Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do dochodzenia lub obrony roszczeń.

§ 5

TECHNICZNE I ORGANIZACYJNE ŚRODKI OCHRONY DANYCH OSOBOWYCH

1. Szpital uwzględniając ryzyko naruszenia praw lub wolności osób fizycznych wdraża odpowiednie środki techniczne i organizacyjne zapewniające stopień bezpieczeństwa odpowiadający temu ryzyku, między innymi poprzez:

- 1) opracowanie procedur,
- 2) określenie zasad dostępu, przetwarzania i udostępniania danych osobowych,
- 3) minimalizowanie ryzyka w obszarze bezpieczeństwa fizycznego, teleinformatycznego, organizacyjno- prawnego oraz osobowego,
- 4) zaangażowanie wszystkich pracowników w ochronę danych osobowych oraz stałe podnoszenie umiejętności i kwalifikacji w tej dziedzinie.

1. ZASADY OBOWIĄZUJĄCE PRZY PRZETWARZANIU DANYCH

- 1) Dane osobowe z użyciem systemu informatycznego i w formie papierowej są przetwarzane w Szpitalu całodobowo.
- 2) Dane osobowe powinny być chronione przed nieuprawnionym dostępem.
- 3) Przebywanie osób nieuprawnionych w pomieszczeniach znajdujących się wewnątrz obszaru przetwarzania danych, jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych.
- 4) Za prawidłowe przechowywanie dokumentacji i ochronę przed osobami nieupoważnionymi odpowiedzialni są wszyscy pracownicy. Sposób i miejsce przechowywania dokumentacji określają kierownicy komórek organizacyjnych Szpitala.
- 5) Dane osobowe zawarte w systemach informatycznych należy przetwarzać wyłącznie za pomocą autoryzowanych programów, dopuszczonych przez ASI/Zespół ds. informatycznych.
- 6) Należy szczególnie chronić dokumenty przenoszone poza obszar przetwarzania danych, poprzez: szyfrowanie danych, używanie zabezpieczonych nośników (np. pendrive'ów z funkcją szyfrowania), transport dokumentów w sposób bezpieczny (np. w zamkniętych kopertach, teczkach).
- 7) Wydruki komputerowe lub dokumenty błędnie sporządzone, zawierające dane osobowe powinny zostać zniszczone tak, aby nie było możliwości odczytania zamieszczonych na nich informacji (np. za pomocą niszczarki dokumentów).
- 8) Dokumenty zawierające dane osobowe, po ustaniu okresu archiwizacji (np. dokumentacja medyczna, akta osobowe), są niszczone w sposób uniemożliwiający ich odtworzenie lub są przekazywane do firmy specjalizującej się w utylizacji dokumentów papierowych/ nośników danych (zgodnie z zawartymi umowami).
- 9) Zabronione jest fotografowanie i filmowanie: systemów zabezpieczeń, pomieszczeń technicznych i pomieszczeń strategicznych (np. serwerowni), nagrywanie dźwięku bez odpowiednich uprawnień czy zgody osób, których te materiały dotyczą.

10) W celu ochrony przed złośliwym oprogramowaniem stosuje się programy antywirusowe, które należy regularnie aktualizować, zgodnie z zaleceniami producenta.

11) W przypadku remontów, nowych projektów (niezależnie od rodzaju projektu), każdorazowo należy uwzględniać infrastrukturę informatyczną i umieszczać ją w projekcie i specyfikacji. Przed rozpoczęciem realizacji danego remontu czy projektu należy poinformować z ASI.

12) ASI ma obowiązek zgłosić zastrzeżenia lub podjąć działania w celu zabezpieczenia sieci.

2. BEZPIECZEŃSTWO OBSZARÓW FIZYCZNYCH

2a. Strefy bezpieczeństwa

W budynkach Szpitala wydziela się trzy strefy bezpieczeństwa:

a) **strefy ogólnodostępne**- na tym terenie może przebywać każdy (pacjenci, interesanci, pracownicy):

- korytarze,
- poczekalnie,
- inne, dostępne dla wszystkich pomieszczenia;

b) **strefy chronione**- na tym terenie mogą przebywać pracownicy oraz inne osoby pod nadzorem pracownika Szpitala:

- pracownie (m. in.: pracownia akceleratorowa, pracownia brachyterapii, pracownia rentgenodiagnostyki, pracownia diagnostyki laboratoryjnej),
- Apteka,
- gabinety lekarskie, gabinety diagnostyczno- zabiegowe,
- dyżurki: lekarskie/pielęgniarskie,
- sekretariaty medyczne,
- pomieszczenia administracyjne/biurowe,
- pomieszczenia ze strategicznymi urządzeniami technicznymi (zbiorniki wody, tlenownie, agregaty prądotwórcze),
- inne do których mają dostęp tylko pracownicy Szpitala;

c) **strefy specjalne (strategiczne)** - na tym terenie mogą przebywać tylko upoważnione osoby lub inne osoby, wyłącznie pod nadzorem pracownika Szpitala:

- serwerownie (każde wejście do serwerowni należy odnotować w Rejestrze wejść/wyjść),
- kasa główna Szpitala,
- archiwum,
- kancelaria tajna.

2b. Dostęp do budynków i pomieszczeń

1. Klucze do budynków mogą pobierać/ posiadać kierownicy komórek organizacyjnych, lub wyznaczeni przez nich pracownicy oraz inni pracownicy Szpitala do wykorzystania do celów służbowych- zgodnie z zakresem czynności lub za zgodą Dyrektora (np. konserwatorzy). Klucze do pomieszczeń pobierane i zdawane są przez wyznaczonych pracowników, w miejscu do tego przeznaczonym.

2. Kierownicy/ Pracownicy posiadający klucz ponoszą pełną odpowiedzialność za należyte zabezpieczenie pomieszczeń w trakcie i po zakończeniu pracy.

3. Kluczy oraz kodów dostępowych do budynków/pomieszczeń służbowych nie wolno udostępniać osobom nieuprawnionym.

Załącznik nr 1 do Zarządzenia nr 79 z dnia 16.06.2025 r.

**POLITYKA BEZPIECZEŃSTWA INFORMACJI I CYBERBEZPIECZEŃSTWA
SZPITALA SPECJALISTYCZNEGO im. JĘDRZEJA ŚNIADECKIEGO
w NOWYM SĄCZU**

4. Klucze od pomieszczeń biurowych, biurek stanowiskowych i szaf biurowych są w posiadaniu Kierowników/Pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie.
5. Pracownik, który posiada klucze do pomieszczenia, przed otwarciem zamków sprawdza czy zamki oraz systemy zabezpieczeń są nienaruszone. W przypadku stwierdzenia zmian lub naruszenia stanu zabezpieczeń; pracownik, który to stwierdzi, powiadamia niezwłocznie o tym fakcie bezpośredniego przełożonego.
6. Zabrania się pracownikom udostępniania kluczy osobom nieupoważnionym i pozostawiania kluczy bez nadzoru.
7. Pracownik, który potrzebuje dodatkowego klucza do pomieszczenia/ budynku szpitala, zobowiązany jest do złożenia pisemnego wniosku do Zespołu ds. administracyjnych. Wniosek ten musi być zatwierdzony przez bezpośredniego przełożonego. We wniosku należy określić, jaki klucz jest wymagany oraz uzasadnić konieczność dostępu do danego pomieszczenia. Wnioskodawca powinien dostarczyć oryginał klucza, w celu umożliwienia wykonania jego kopii.
8. Po zakończeniu dnia pracy, pracownicy zobowiązani są do uporządkowania swoich stanowisk pracy:
 - zabezpieczenia dokumentacji i pieczęci służbowych,
 - zabezpieczenia/ wyłączenia komputerów, nośników danych oraz wszelkich urządzeń elektronicznych będących częścią struktury teleinformatycznej szpitala,
 - wyłączenia wszystkich urządzeń zasilanych energią elektryczną (czajniki, wentylatory itp.),
 - zamknięcia biurek/ szaf/ okien/ drzwi wejściowych.
9. W przypadku zagubienia/zaginięcia klucza, należy niezwłocznie poinformować bezpośredniego przełożonego i podjąć odpowiednie działania w celu zabezpieczenia dostępu (np. wymianę zamków). Pracownik, może zostać obciążony kosztami wymiany zamków lub wkładek do drzwi, jeśli ponosi odpowiedzialność za zagubienie klucza.
10. Klucze do nowo wybudowanych/oddawanych do użytkowania budynków/ pomieszczeń odbiera Koordynator Zespołu ds. administracyjnych, który odpowiada za:
 - ponumerowanie/ opisanie/ oznakowanie brelokami wszystkich kluczy,
 - utworzenie min. 3 kompletów kluczy, które:
 - 1 komplet przekazuje kierownikowi komórki organizacyjnej,
 - 1 komplet zabezpiecza w depozycie,
 - 1 komplet pozostaje w dyspozycji Koordynatora Zespołu ds. administracyjnych do czasu pełnego wyposażenia i uruchomienia danej komórki organizacyjnej. Po wykorzystaniu komplet jest przekazywany kierownikowi komórki organizacyjnej, przez którego jest zabezpieczony w komórce organizacyjnej- jako klucz zapasowy.
11. Kierownik komórki organizacyjnej przynajmniej 1 raz w roku dokonuje przeglądu zabezpieczonych kluczy zapasowych pod kątem ich dalszej przydatności. Klucze zbędne są wycofywane z użytkowania.
12. W przypadku wymiany drzwi/ zamków, należy zabezpieczyć nowe klucze/ komplety kluczy zapasowych, jak przy odbiorze budynku.
13. Po rozwiązaniu umowy/ współpracy ze szpitalem, pracownik zobowiązany jest do zwrotu bezpośredniemu przełożonemu, wszelkich posiadanych kluczy dostępowych do budynków/ pomieszczeń (w tym np. chipów dostępowych do wind, kart do terminali, kart do ewidencji czasu pracy).
14. Zobowiązuje się wszystkich pracowników do:
 - zwracania uwagi na zachowanie osób wchodzących i wychodzących,

Załącznik nr 1 do Zarządzenia nr 79 z dnia 16.06.2025 r.
POLITYKA BEZPIECZEŃSTWA INFORMACJI I CYBERBEZPIECZEŃSTWA
SZPITALA SPECJALISTYCZNEGO im. JĘDRZEJA ŚNIADECKIEGO
w NOWYM SĄCZU

- reagowania na wejście do pomieszczeń i budynków osób nie będących pracownikami,
- reagowania na próby wnoszenia/ wwożenia na teren Szpitala przedmiotów niebezpiecznych, materiałów lub substancji budzących podejrzenie itp.,
- natychmiastowego reagowania, poprzez powiadomienie odpowiednich służb oraz osób o zaobserwowanych próbach stworzenia zagrożenia dla życia i zdrowia, a także utraty lub niszczenia mienia. W takiej sytuacji należy każdorazowo wezwać załogę interwencyjną- nr tel. 618.

2c. Postępowanie z kluczami zapasowymi do budynków/pomieszczeń

1. Tworzy się dodatkowo komplet kluczy do wykorzystania w sytuacjach nagłych/ szczególnych (np. pożar, zalanie, awaria), aby osoby upoważnione miały do nich dostęp.
2. Klucze zapasowe do budynków/ pomieszczeń przechowywane są w budynku Dyrekcji.
3. Klucze zapasowe mogą być pobrane wyłącznie na polecenie Dyrektora lub osoby wskazanej przez Dyrektora.

2d. Wstęp do pomieszczeń strategicznych i serwerowni

1. Wstęp do pomieszczeń strategicznych, jest ściśle ograniczony do upoważnionych pracowników.
2. Każdorazowe wejście do serwerowni, na czas niezbędny na wykonanie prac (przez pracowników szpitala, pracowników firm zewnętrznych- np. w celu wykonania określonych w umowach prac; innych osób (np. osoby kontrolujące) dopuszczalne jest jedynie w obecności i pod nadzorem Koordynatora Zespołu ds. informatycznych lub wyznaczonego przez niego informatyka.
3. Każde wejście do serwerowni należy odnotować w rejestrze wejść/wyjść do serwerowni. Rejestr ten zawiera: datę i godzinę wejścia/ wyjścia, imię i nazwisko wchodzącego, stanowisko, nazwę firmy (jeśli dotyczy), cel wejścia do pomieszczenia.
4. W nagłych sytuacjach (np. pożar, zalanie, awaria sprzętu), dostęp musi zostać udzielony natychmiastowo- wyłącznie osobom przeszkolonym w zakresie reagowania na sytuacje kryzysowe (np. personel odpowiedzialny za zarządzanie kryzysowe, strażacy).

2e. Dostęp do budynków/pomieszczeń przez pracowników i personel sprzątający

1. Klucze zapasowe do pomieszczeń znajdują się w wyznaczonym budynku.
2. Osoba, która pobrała klucze, ponosi pełną odpowiedzialność za właściwe użytkowanie i zabezpieczenie kluczy i nie może udostępniać kluczy innym pracownikom/osobom.
3. Każdorazowe pobranie i zwrot kluczy do pomieszczeń przez personel sprzątający, należy odnotować w rejestrze (data i godzina pobrania/ zwrotu, podpis osoby pobierającej/zwracającej klucze).
4. Po zakończonej pracy personel sprzątający ponosi odpowiedzialność za zamknięcie okien oraz drzwi wewnętrznych i wejściowych do budynków jak również za zwrot kluczy.
5. Pomieszczenia podlegające szczególnej ochronie oraz pomieszczenia strategiczne są sprzątane w godzinach normalnej pracy w obecności pracownika komórki organizacyjnej.

3. KORZYSTANIE Z SAMOCHODÓW SŁUŻBOWYCH I PRYWATNYCH

3a. Korzystanie z samochodów służbowych przez pracowników Szpitala.

1. Samochody służbowe używane są przez pracowników Szpitala wyłącznie w celach służbowych.
2. Kierować samochodem służbowym mogą tylko wyznaczeni pracownicy, posiadający stosowne uprawnienia.
3. Po zakończeniu pracy samochody służbowe powinny być zaparkowane w wyznaczonych miejscach na terenie Szpitala.

Załącznik nr 1 do Zarządzenia nr 79 z dnia 16.06.2025 r.
POLITYKA BEZPIECZEŃSTWA INFORMACJI I CYBERBEZPIECZEŃSTWA
SZPITALA SPECJALISTYCZNEGO im. JĘDRZEJA ŚNIADECKIEGO
w NOWYM SĄCZU

4. Po zakończeniu pracy dowód rejestracyjny wraz z kluczami do samochodu służbowego należy pozostawić w Sekretariacie Dyrekcji lub u kierownika komórki organizacyjnej.
5. Pracownik korzystający z samochodu służbowego zobowiązany jest do utrzymania samochodu w czystości oraz do dokonywania bieżących przeglądów.
6. Pracownik ponosi pełną odpowiedzialność za użytkowanie samochodu zgodnie z przepisami i jego właściwe zabezpieczenie.
7. Samochodu służbowego nie wolno udostępniać osobom nieupoważnionym.
8. Wyznaczony pracownik Zespołu ds. administracyjnych odpowiada za terminowe: dokonywanie opłat obowiązkowego ubezpieczenia oraz przeprowadzanie obowiązkowych okresowych przeglądów technicznych.

3b. Używanie prywatnego samochodu osobowego do celów służbowych

1. Do celów służbowych może być wykorzystywany prywatny samochód osobowy stanowiący własność (współwłasność) pracownika, lub będący w jego dyspozycji (np. na podstawie umowy najmu, użyczenia, leasingu).
2. Dyrektor Szpitala może wyrazić zgodę na użycie samochodu prywatnego pracownika do celów służbowych.
3. Podróże służbowe z wykorzystaniem samochodu prywatnego pracownika odbywają się na podstawie polecenia wyjazdu służbowego (np. delegacji) lub polecenia Dyrektora.
4. Koszty użycia prywatnego samochodu pracownika do celów służbowych pokrywa pracodawca na zasadach określonych w obowiązujących przepisach.

4. OCHRONA PRZY ZBIERANIU I PRZEKAZYWANIU DANYCH

1. Przy rejestracji oraz w pomieszczeniach, gdzie są udzielane informacje (administracyjnych, sekretariatach, dyżurkach medycznych) powinna znajdować się tylko osoba załatwiająca sprawę.
2. Rejestracji pacjentów należy dokonywać tak, aby zapewnić anonimowość, poprzez zastosowanie wybranych rozwiązań, np.:
 - weryfikacja danych pacjenta poprzez odczytanie jego danych z dokumentu tożsamości lub danych przekazanych przez pacjenta na piśmie,
 - zamieszczenie komunikatu o konieczności przebywania przy stanowisku jednej osoby,
 - taśmy/ bariery wyznaczające obszar, w którym może przebywać obsługiwana osoba,
 - oddzielenie strefy rejestracji: ścianką, szybą, taśmą, barierką,
 - wprowadzenie odpowiedniej odległości między stanowiskami,
 - utworzenie rejestracji w osobnym pomieszczeniu, poza korytarzem/ miejscem oczekujących,
 - rejestracja telefoniczna/ elektroniczna (np. e-rejestracja).
3. Za wprowadzenie odpowiedniego rozwiązania odpowiada kierownik komórki organizacyjnej.
4. Pacjentów należy wzywać do gabinetów, m. in.: na podstawie numeru nadanego podczas rejestracji lub po godzinie wizyty lub w inny sposób zapewniający anonimowość.
5. W Szpitalnym Oddziale Ratunkowym stosowany jest system kolejkowy z elektroniczną tablicą wyświetlającą numery.
6. W przypadkach szczególnych (zagrożenia zdrowia lub życia) możliwe jest zastosowanie metody identyfikacji tożsamości pacjenta z wykorzystaniem imienia i nazwiska.
7. W pomieszczeniach, do których dostęp mają osoby postronne, dokumentacja zawierająca dane, w tym dane osobowe powinna być zabezpieczona przed podglądnięciem, zabraniem czy zrobieniem zdjęć (np. zamykane biurka/ szafy, segregatory, zasłonięcie/ odwrócenie dokumentu niezapisaną stroną).

5. UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby, które otrzymały upoważnienie do przetwarzania danych podpisane przez Dyrektora (AD)- **Załącznik nr 2 do PBliC**, zostały przeszkolone z zasad ochrony danych osobowych oraz podpisały stosowne oświadczenie o zachowaniu w tajemnicy przetwarzanych danych osobowych- **Załącznik nr 3 do PBliC**.
2. Dostęp do danych osobowych jest przyznawany zgodnie z:
 - zasadą wiedzy koniecznej- pracownicy posiadają wiedzę o zasobach Szpitala ograniczoną wyłącznie do zagadnień, które są potrzebne do realizacji powierzonych zadań.
 - zasadą indywidualnej odpowiedzialności- wszyscy pracownicy są świadomi indywidualnej odpowiedzialności i konsekwencji, za zaniedbanie obowiązków w zakresie ochrony danych.
3. Upoważnienia są nadawane indywidualnie przed rozpoczęciem przetwarzania danych osobowych:
 - do dokumentacji papierowej (w części: medycznej-białej lub administracyjnej- szarej),
 - do systemów informatycznych (system, moduł, schemat, zakres/poziom dostępu).
4. Wydanie upoważnienia oraz rejestracja użytkownika systemu informatycznego przetwarzającego dane osobowe następuje na podstawie Karty obiegowej- zatrudnienia lub wniosku bezpośredniego przełożonego.
5. Upoważnienia oraz oświadczenia, sporządza się w 2 egzemplarzach: 1 egzemplarz dla upoważnionego pracownika, 1 egzemplarz przechowuje się w dokumentacji pracownika.
6. W uzasadnionych przypadkach przetwarzać dane osobowe w systemach informatycznych mogą na wniosek bezpośredniego przełożonego/opiekuna; praktykanci, stażyści, wolontariusze, osoby odbywające staże specjalizacyjne w szpitalu.
7. IOD wraz z ASI/LAS jest zobowiązany do prowadzenia Rejestru osób upoważnionych do przetwarzania danych osobowych w poszczególnych systemach.

6. DOSTĘP DO SIECI I SYSTEMÓW INFORMATYCZNYCH DLA UŻYTKOWNIKÓW

1. Każdy pracownik jest zobowiązany do korzystania z systemów informatycznych wyłącznie przy użyciu indywidualnego konta użytkownika, które zostało mu przydzielone na podstawie upoważnienia do przetwarzania danych.
2. Udostępnianie danych do logowania w systemach (login i hasło) innym osobom jest zabronione.
3. W celu ochrony przed nieautoryzowanym dostępem, systemy informatyczne powinny posiadać mechanizm automatycznej blokady konta użytkownika po określonej liczbie nieudanych prób logowania (w systemie Eskulap trzy błędne próby logowania, blokują dostęp do systemu).
4. Blokada konta użytkownika ma charakter tymczasowy, może być zniesiona wyłącznie przez uprawnionego administratora systemu.
5. Rejestry dotyczące prób logowania muszą być przechowywane w systemie i dostępne do wglądu administratora, w celach audytowych oraz analizy incydentów bezpieczeństwa.

7. NADAWANIE UPRAWNIEŃ DO SYSTEMÓW INFORMATYCZNYCH DLA INFORMATYKA

1. Uprawnienia nadawane informatykowi w systemach informatycznych przyznaje się, w zależności od zakresu czynności i odpowiedzialności:
 - dostęp użytkownika standardowego- dostęp do aplikacji i systemów niezbędnych do wykonywania codziennych obowiązków. Uprawnienia do odczytu i/lub wprowadzania danych w zakresie stanowiska.

Załącznik nr 1 do Zarządzenia nr 79 z dnia 16.06.2025 r.
POLITYKA BEZPIECZEŃSTWA INFORMACJI I CYBERBEZPIECZEŃSTWA
SZPITALA SPECJALISTYCZNEGO im. JĘDRZEJA ŚNIADECKIEGO
w NOWYM SĄCZU

- dostęp administratora- dostęp do systemów umożliwiających konfigurację aplikacji, serwerów, baz danych oraz zarządzanie użytkownikami. Uprawnienia do zarządzania systemami, instalacji oprogramowania i aktualizacji.
 - dostęp superużytkownika (root)- pełny dostęp do wszystkich systemów i aplikacji, umożliwiający m.in. zmiany w konfiguracji systemów operacyjnych, dostęp do poufnych danych oraz pełną kontrolę nad środowiskiem IT.
2. Wniosek o przydzielenie dostępów do systemów informatycznych dla stażysty/ praktykanta w Zespole ds. informatycznych składa do AD, Koordynator zespołu.

8. DOSTĘP DO PLATFORMY MAŁOPOLSKI SYSTEM INFORMACJI MEDYCZNEJ /MSIM/

1. Personel medyczny, który otrzymuje dostęp do systemu Eskulap; po podpisaniu stosownego oświadczenia o zapoznaniu z Polityką Bezpieczeństwa dla Partnerów; uzyskuje odpowiednie uprawnienia do Platformy Małopolskiego Systemu Informacji Medycznej (dalej: MSIM).
2. Informatycy tworząc konta do platformy MSIM, podają następujące dane: imię, nazwisko, numer prawa wykonywania zawodu, e-mail, nazwę użytkownika, część pierwszą kodu resortowego; oraz wskazują rolę użytkownika w MSIM.

9. ZARZĄDZANIE HASŁAMI DO SYSTEMÓW INFORMATYCZNYCH

1. Dostęp do systemu informatycznego może posiadać użytkownik po podaniu loginu i hasła.
2. Za przydzielenie i wygenerowanie loginu oraz hasła użytkownikowi, który pierwszy raz będzie korzystał z systemu informatycznego odpowiada Zespół ds. informatycznych/ LAS odpowiedniego systemu informatycznego.
3. Hasło ustanowione podczas przyznawania uprawnień należy zmienić na indywidualne po pierwszym poprawnym zalogowaniu się do systemu. Zmiany haseł nie wolno zlecać innym osobom.
4. Hasła dostępowe do systemu informatycznego (z wyjątkiem haseł startowych) tworzone są przez użytkownika i stanowią tajemnicę znaną danemu użytkownikowi.
5. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
6. Pracownicy są odpowiedzialni za zachowanie w poufności swoich loginów i haseł.
7. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło, pracownik zobowiązany jest do natychmiastowej zmiany hasła i poinformowania o tym fakcie IOD i ASI/LAS.
8. Przy wyborze hasła obowiązują następujące zasady:
 - minimalna długość hasła **15 znaków** (dopuszcza się mniejszą ilość znaków w hasłach dostępu, gdzie występują ograniczenia programowe),
 - złożoność hasła: hasło powinno zawierać kombinacje: dużych i małych liter, cyfr, znaków specjalnych (np.,(,):'@, #, & itp.)- jeżeli system informatyczny na to pozwala;
 - tworząc silne hasło, można użyć zdania lub frazy, które jest łatwe do zapamiętania dla użytkownika, a jednocześnie trudne do złamania - jeśli zostaną dodane znaki specjalne, cyfry oraz wielkie litery,
 - w przypadku systemów informatycznych, które nie wymuszają automatycznie cyklicznej zmiany hasła, obowiązkiem użytkownika jest zmiana hasła **minimum co 90 dni**.
9. Zabrania się tworzenia haseł na podstawie:
 - a) cech i informacji związanych z użytkownikiem (np. m.in. dat urodzenia, imion, nazwisk, numerów telefonów, przezwisk zwierząt),
 - b) sekwencji klawiszy klawiatur (np. qwerty, 12qwaszx),

Załącznik nr 1 do Zarządzenia nr 79 z dnia 16.06.2025 r.
POLITYKA BEZPIECZEŃSTWA INFORMACJI I CYBERBEZPIECZEŃSTWA
SZPITALA SPECJALISTYCZNEGO im. JĘDRZEJA ŚNIADECKIEGO
w NOWYM SĄCZU

- c) identyfikatora użytkownika w jakiejkolwiek formie,
 - d) ogólnie dostępnych informacji o użytkowniku (np. numer telefonu, numer rejestracyjny samochodu, itp.),
 - e) nazw miesięcy, pór roku itp. (np. Sierpień2023, czerwiec2021),
 - f) opartych na pojedynczych słowach występujących w słownikach językowych (np. *Onomatopeja13@*, *Hasło123*, *Password!*, itp.), nawet jeśli zostały dodane cyfry lub znaki specjalne.
10. Ponadto zabrania się:

- a) zapisywania haseł i pozostawiania ich w widocznym/ ogólnodostępnym miejscu,
- b) korzystania z funkcji zapamiętywania hasła- pracownicy są zobowiązani do unikania zapamiętywania haseł do systemów/kont służbowych w sposób, który nie zapewnia odpowiedniego poziomu ochrony. Hasła nie mogą być zapamiętywane w sposób niekontrolowany, np. w pamięci podręcznej przeglądarek, w notatkach, ani w żaden sposób, który może narazić je na ujawnienie. Wszystkie hasła do systemów powinny być przechowywane w bezpiecznych, szyfrowanych narzędziach, takich jak menedżer haseł.
- c) wpisywania haseł „na stałe” (np. w telefonie komórkowym, przeglądarkach www),
- d) wykorzystywania domyślnych („fabrycznych”) haseł,
- e) używania tych samych haseł w różnych systemach operacyjnych i aplikacjach,
- f) przekazywania haseł innym osobom.

11. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.

12. Po zakończeniu pracy należy wylogować się z wszystkich programów i aplikacji oraz wyłączyć komputer.

13. Przegląd uprawnień użytkowników w systemach (zakresy i poziomy dostępu) realizowany jest okresowo; przez IOD i ASI wraz z kierownikiem komórki organizacyjnej.

14. Pracownik/ bezpośredni przełożony pracownika/ Koordynator Zespołu ds. Zatrudnienia i Płac (osobiście, telefonicznie, przez rejestr zgłoszeń do Zespołu IT), jest zobowiązany zgłosić potrzebę zmiany dostępu do przetwarzanych danych dla pracownika w przypadku zmiany komórki organizacyjnej- np. oddelegowania, zastępstwa.

10. WYREJESTROWANIE UŻYTKOWNIKA Z SYSTEMU INFORMATYCZNEGO

1. Wyrejestrowanie użytkownika z systemu informatycznego/ zablokowanie uprawnień do przetwarzania danych w systemie może nastąpić:

- a) na podstawie Karty obiegowej- zwolnienia (rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego),
- b) na wniosek AD, bezpośredniego przełożonego (także telefonicznie),
- c) w przypadku zawieszenia w pełnieniu obowiązków służbowych,
- d) z uwagi na inne istotne okoliczności.

2. Login użytkownika, który utracił uprawnienia do przetwarzania danych nie może być przydzielony innej osobie.

3. Login użytkownika ponownie zatrudnianego w Szpitalu, może pozostać taki sam jak w poprzednim zatrudnieniu. Przed ponownym aktywowaniem IOD przeprowadza weryfikację uprawnień z bezpośrednim przełożonym pracownika, informatyk przeprowadza zmianę haseł oraz dostosowuje dostęp do zakresu czynności pracownika.

11. MONITOROWANIE DZIAŁAŃ UŻYTKOWNIKÓW W SYSTEMACH INFORMATYCZNYCH

1. Kluczowe działania użytkowników w systemach informatycznych są rejestrowane i monitorowane.

12. UWIERZYTELNIANIE WIELOSKŁADNIKOWE (MFA)

1. Zdalny dostęp do systemów informatycznych szpitala, realizowany spoza sieci wewnętrznej, musi być zabezpieczony uwierzytelnianiem wieloskładnikowym (MFA).

13. UŻYTKOWANIE URZĄDZEŃ DO PRZETWARZANIA DANYCH

1. Wszelkie dane wytworzone przez pracowników na urządzeniach służbowych stanowią własność Szpitala.

2. Urządzenia i sprzęt informatyczny służący do przetwarzania danych jest przypisany do konkretnej komórki organizacyjnej/ stanowiska.

3. Odpowiedzialność za sprzęt z którego korzysta pracownik w czasie pracy jest przypisana pracownikowi, który jest zobowiązany do dbałości o powierzone mu urządzenia oraz zapewnienie ich odpowiedniego użytkowania i zabezpieczenia w trakcie ich wykorzystywania (np. przed kradzieżą, uszkodzeniem, utratą danych).

4. Komputery, dyski lub nośniki wymienne, przeznaczone do przekazania (np. do naprawy, sprzedaży), należy pozbawić zapisanych danych, w sposób uniemożliwiający ich odzyskanie- czynności te wykonuje informatyk lub inna osoba (np. pracownik firmy zewnętrznej- przy udziale informatyka).

5. Komputery, dyski lub nośniki wymienne lub przeznaczone do likwidacji należy pozbawić zapisanych danych, w sposób uniemożliwiający ich odzyskanie; jeżeli nie jest to możliwe uszkadza się je w sposób uniemożliwiający ich odczytanie i wycofuje z użytkowania- czynności te wykonuje ASI lub wyznaczony informatyk, który wydaje protokół potwierdzający trwałe usunięcie danych.

6. Użytkownik ma obowiązek zwrócić przypisane do niego urządzenia: na polecenie bezpośredniego przełożonego lub ostatniego dnia pracy (w przypadku zakończenia zatrudnienia).

13a. Użytkowanie służbowych i prywatnych urządzeń przenośnych (np. laptop, notebook)

1. Użytkownik jest zobowiązany do należytej ochrony służbowych i prywatnych urządzeń przenośnych wykorzystywanych do celów służbowych, w szczególności przed: uszkodzeniem, kradzieżą, zagubieniem; dostępem osób nieuprawnionych.

2. Urządzenia muszą być zabezpieczone (np. hasłem, kodem). Ekran powinien automatycznie blokować się po określonym czasie bezczynności.

3. Użycie prywatnego laptopa lub innego urządzenia do celów służbowych jest dozwolone wyłącznie po uzyskaniu zgody AD i spełnieniu określonych wymagań bezpieczeństwa określonych przez Zespół ds. informatycznych (np. zainstalowany program antywirusowy, aktualny system operacyjny, VPN).

4. Laptopy i inne urządzenia przenośne należy transportować w odpowiednich torbach ochronnych, zabezpieczających je przed wstrząsami, zarysowaniami i innymi uszkodzeniami mechanicznymi.

5. Urządzenia nie mogą być pozostawiane bez nadzoru w miejscach publicznych lub bez właściwego zabezpieczenia (szafa zamykana na klucz).

6. Użytkownik zobowiązany jest do regularnego instalowania aktualizacji systemu operacyjnego i oprogramowania. Instalowanie nieautoryzowanych programów jest zabronione.

13b. Korzystanie z telefonu służbowego

1. Telefony stacjonarne oraz komórkowe mogą być wykorzystywane przez użytkowników do celów służbowych.
2. W przypadku telefonów komórkowych obligatoryjne jest stosowanie blokady ekranu.

13c. Korzystanie z przenośnych nośników pamięci

1. Porty USB są domyślnie zablokowane- użytkownik nie ma możliwości samodzielnego podłączenia i użycia urządzeń przenośnych.
2. Dopuszcza się wykorzystywanie służbowych przenośnych nośników pamięci, które zostały zaszyfrowane przez informatyków.
3. Zespół ds. informatycznych monitoruje próby podłączenia urządzeń zewnętrznych do komputerów służbowych.

13d. Wykonywanie przeglądów urządzeń UPS

1. Przeglądy, konserwacja, zapewnienie gotowości do pracy UPS-ów wykonywane są przez elektryków Zespołu ds. technicznych lub pracowników firmy zewnętrznej z uprawnieniami (dotyczy UPS-ów w rozdzielniach głównych budynków oraz UPS-ów do celów medycznych)- 1 x w roku. Pozostałe UPS'y podlegają przeglądowi przez informatyków- 1 x kwartał.
2. Wszystkie przeglądy oraz czynności serwisowe powinny być udokumentowane (np. w protokołach, rejestrach, kartach przeglądu) i powinny zawierać m. in.: datę przeglądu/ serwisu, dane identyfikacyjne UPS (model, numer seryjny, lokalizacja), zakres wykonanych czynności, imię i nazwisko osoby wykonującej przegląd, wynik przeglądu (np. dopuszczenie do eksploatacji lub zalecenia naprawcze), uwagi i zalecenia eksploatacyjne.
3. Testy awaryjne UPS-ów przeprowadza ASI lub wyznaczony informatyk w porozumieniu z elektrykiem.

14. ZABEZPIECZENIE SYSTEMU INFORMATYCZNEGO PRZED DZIAŁALNOŚCIĄ SZKODLIWEGO OPROGRAMOWANIA

1. System informatyczny zabezpiecza się programem antywirusowym.
2. Instalacji i aktualizacji programu antywirusowego, dokonuje Koordynator Zespołu ds. Informatycznych lub osoba go zastępująca.
3. Użytkownicy są zobowiązani, do natychmiastowego zgłaszania podejrzenia zainfekowania komputera do Zespołu ds. informatycznych.
4. Informatycy podejmują działania zmierzające do usunięcia zagrożenia za pomocą dostępnych narzędzi.
5. Wyłączanie antywirusa jest bezwzględnie zabronione i może skutkować wyciągnięciem konsekwencji służbowych/ dyscyplinarnych.

15. WYKONYWANIE PRZEGŁĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH

1. Przeglądy i konserwacje urządzeń zawierających dane osobowe lub służące do świadczenia usług kluczowych powinny być wykonywane w terminach określonych przez producenta sprzętu lub zgodnie z potrzebami.
2. Prace serwisowe urządzeń zawierających dane osobowe mogą być wykonywane wyłącznie przez pracowników Szpitala (informatycy, pracownicy aparatury medycznej) lub przez upoważnionych przedstawicieli wykonawców zewnętrznych pracujących pod nadzorem

Załącznik nr 1 do Zarządzenia nr 79 z dnia 16.06.2025 r.

**POLITYKA BEZPIECZEŃSTWA INFORMACJI I CYBERBEZPIECZEŃSTWA
SZPITALA SPECJALISTYCZNEGO im. JĘDRZEJA ŚNIADECKIEGO
w NOWYM SĄCZU**

pracowników Szpitala. Imienne upoważnienia dla osób dokonujących przeglądów są nadawane w oparciu o obowiązujące umowy. W przypadku aparatów dzierżawionych za wystąpienie do AD o nadanie upoważnień oraz weryfikację tożsamości serwisantów odpowiada kierownik komórki organizacyjnej, gdzie znajduje się aparat/urządzenie.

3. Prace serwisowe/aktualizacyjne powinny w miarę możliwości odbywać się, tak aby nie zakłócać pracy danej komórki (po uzgodnieniu z jej kierownikiem).

4. Kierownik komórki organizacyjnej nadzoruje lub wskazuje osobę odpowiedzialną za nadzór nad serwisantami dokonującymi przeglądów/serwisów.

5. Zespół ds. technicznych informuje kierownika danej komórki, o wizycie serwisanta oraz przekazuje dane osób/dane firmy, które będą realizować prace.

6. Przed rozpoczęciem prac serwisowych przez wykonawców zewnętrznych konieczne jest potwierdzenie tożsamości serwisantów przez pracownika udostępniającego urządzenie do przeglądu/konserwacji/naprawy.

7. Serwisant powinien posiadać przy sobie ważny dokument pozwalający na zweryfikowane jego tożsamości.

8. W przypadku wątpliwości dotyczących tożsamości serwisanta lub nieprawidłowego przebiegu procesu weryfikacji, pracownik szpitala nie udostępnia urządzenia i natychmiast zgłasza sytuację bezpośredniemu przełożonemu i IOD.

16. KORZYSTANIE Z INTERNETU I KOMUNIKATORÓW INTERNETOWYCH

1. Pracownik ma prawo korzystać z sieci Internet Szpitala, zgodnie z prawem, wyłącznie w celach związanych z realizacją zadań służbowych w zakresie przyznaných uprawnień.

2. Odpowiedzialność za szkody spowodowane pobieraniem z sieci nielegalnych programów lub plików z niewiadomego źródła ponosi pracownik.

3. W celu ochrony sieci teleinformatycznej blokuje się dostęp do sieci Internet na stanowiskach terminalowych z wyłączeniem stron niezbędnych do wykonywania czynności służbowych, po uzyskaniu zgody Dyrektora.

4. Zabrania się korzystania z portali społecznościowych, np.: Messenger, Gadu-Gadu, Skype, WhatsApp itp., do przetwarzania danych w celach służbowych.

17. KORZYSTANIE ZE SŁUŻBOWEJ POCZTY ELEKTRONICZNEJ

1. Pracownikom nadaje się dostęp do służbowej poczty elektronicznej (ogólny- dla danej komórki organizacyjnej lub indywidualny- imienny przypisany do danego pracownika- użytkownika).

2. Adres konta pocztowego jest tworzony wg stałego wzorca dla wszystkich kont.

3. Poczte służbową wykorzystuje się do celów służbowych.

4. Pracownik przysyłając informacje za pośrednictwem poczty, ponosi odpowiedzialność za prawidłowe zaadresowanie wiadomości i przesłanie do uprawnionego odbiorcy.

5. W przypadku wysyłania wiadomości do wielu odbiorców ich adresy e-mail należy umieścić w polu DW (do wiadomości) lub UDW (ukryte do wiadomości).

6. Pracownicy ponoszą odpowiedzialność za działania podejmowane z wykorzystaniem przydzielonego konta pocztowego.

7. Każda korespondencja wysyłana przez użytkownika powinna zawierać:

- stopkę zawierającą dane identyfikujące pracownika,
- klauzulę informacyjną.

Załącznik nr 1 do Zarządzenia nr 79 z dnia 16.06.2025 r.
POLITYKA BEZPIECZEŃSTWA INFORMACJI I CYBERBEZPIECZEŃSTWA
SZPITALA SPECJALISTYCZNEGO im. JĘDRZEJA ŚNIADECKIEGO
w NOWYM SĄCZU

8. Hasło do zaszyfrowanej wiadomości musi być wysyłane przez użytkownika do odbiorcy oddzielnym kanałem komunikacji od tego, którym został wysłany załącznik lub wiadomość (np. telefonicznie, sms). Ze stałymi kontrahentami można ustalić stałe hasło z jego okresową zmianą.
9. Nie należy otwierać korespondencji (w tym załączników), w sposób oczywisty nie związanej z pełnionymi obowiązkami.
10. Należy zwracać uwagę na otwierane załączniki, jeśli wydają się podejrzane, nie należy ich otwierać, tylko przesłać wiadomość z plikiem do Zespołu ds. informatycznych w celu jego weryfikacji.
11. Zabrania się przesyłania za pośrednictwem poczty elektronicznej treści niezgodnych z obowiązującymi przepisami prawa, naruszających zasady współżycia społecznego oraz naruszających prawa własności intelektualnej innych osób.
12. Zabrania się przesyłania załączników zawierających pliki zagrażające lub mogące zagrażać bezpieczeństwu systemu teleinformatycznego Szpitala.
13. Użytkownikom zabrania się wysłać wiadomości służbowe na prywatne adresy e-mail oraz prywatne na służbowe adresy e-mail.
14. Kontrola wolnego miejsca w służbowej skrzynce pocztowej w ramach przyznanej przestrzeni dyskowej leży po stronie użytkownika.
15. Wiadomości, które nie wymagają przechowywania w celu ich przyszłego wykorzystania powinny być regularnie usuwane ze skrzynki pocztowej.
16. Pracodawca może wprowadzić kontrolę służbowej poczty elektronicznej pracownika.
17. Dostęp do poczty służbowej przyznaje się na okres zatrudnienia w szpitalu. Pracownik przed wygaśnięciem umowy powinien: posegregować wiadomości, usunąć niepotrzebne wątki i korespondencję, przekazać korespondencję oraz informacje kluczowe osobie, która przejmuje obowiązki.

18. UDZIELANIE INFORMACJI TELEFONICZNIE

1. Każdorazowo należy potwierdzić tożsamość osoby kontaktującej się, jako osoby uprawnionej do otrzymania informacji, poprzez zadanie dodatkowych pytań kontrolnych dotyczących danych pacjenta, które mogą potwierdzić jego tożsamość (np. imię, nazwisko, numer PESEL, data urodzenia).
2. Przed udzieleniem jakiegokolwiek informacji dotyczącej stanu zdrowia pacjenta, należy upewnić się, że osoba dzwoniąca jest uprawniona do jej otrzymania.
3. Zasady udzielania informacji telefonicznie ujęto w Wytycznych w sprawie realizacji przez osoby uprawnione prawa do informacji o stanie zdrowia pacjentów na odległość, opracowanych przez Rzecznika Praw Pacjenta (dostępne na serwerze Szpitala).

19. POZOSTAWIANIE ULOTEK/PLAKATÓW/BROSZUR/MATERIAŁÓW REKLAMOWYCH I EDUKACYJNYCH NA TERENIE SZPITALA I WYDAWANIE ZGÓD DLA PRZEDSTAWICIELI HANDLOWYCH I FIRM

1. Firmy, które chcą prowadzić na terenie szpitala promocję leków, spotkania edukacyjne, pozostawiać materiały promocyjne i edukacyjne itp. muszą uzyskać zgodę Dyrektora oraz uzgodnić termin wizyty, zgodnie z Zarządzeniem Dyrektora w sprawie ustalenia zasad organizacji spotkań z przedstawicielami medycznymi lub handlowymi w celu reklamy produktów.
2. Pacjenci nie mogą być zmuszeni do przyjęcia materiałów promocyjnych czy udziału w spotkaniach/szkoleniach/wydarzeniach promocyjnych.

20. CZYSTE BIURKO I EKRAN

1. Każdy pracownik zobowiązany jest do przestrzegania zasad czystego biurka i ekranu.
2. Zasada czystego biurka zobowiązuje do utrzymywania porządku w miejscu pracy. Na biurku powinny znajdować się tylko dokumenty, które są w danej chwili niezbędne do wykonywania bieżącej pracy. Dokumenty niewykorzystywane w bieżącej pracy powinny znajdować się w miejscach do tego przeznaczonych, np. szafach i szufladach zamykanych na klucz.
3. Ekran monitora powinien być tak ustawiony, aby uniemożliwić osobom niepowołanym jego podgląd.
4. Monitory komputerów powinny mieć włączony wygaszacz ekranu.

21. OCHRONA DANYCH W KONTAKTACH Z MEDIAMI

1. Kontakt z mediami mają osoby wyznaczone przez Dyrektora.
2. Informacje przekazywane publicznie nie mogą naruszać przepisów prawa dot. ochrony danych osobowych.

22. WYKORZYSTYWANIE PODPISÓW I CERTYFIKATÓW ELEKTRONICZNYCH

1. Zakupione przez Szpital podpisy oraz certyfikaty elektroniczne są jego własnością.
2. Użytkownik ma prawo i obowiązek stosować udostępnione mu podpisy oraz certyfikaty do zadań służbowych.

23. POSTĘPOWANIE W PRZYPADKU AWARII/ AKTUALIZACJI SYSTEMU INFORMATYCZNEGO

1. W razie wystąpienia awarii systemu informatycznego, należy niezwłocznie zgłosić ją do Zespołu ds. informatycznych.
2. W przypadku braku zasilania użytkownik ma obowiązek niezwłocznie bezpiecznie zakończyć pracę i wyłączyć stację roboczą.
3. W przypadku dokonywanej aktualizacji systemów, komórki organizacyjne z wyprzedzeniem zostają informowane (pismo, e-mail) o jej przeprowadzeniu (data, godziny aktualizacji, opis postępowania). Informację jest obowiązany przekazać pracownikom Koordynator Zespołu ds. informatycznych lub wyznaczony informatyk.
4. Do czasu usunięcia awarii/ przywrócenia pełnej funkcjonalności systemu informatycznego, wszystkie operacje i procesy, które normalnie były wykonywane za pomocą tego systemu, są prowadzone w wersji papierowej.
5. Za zaopatrzenie w druki dokumentacji papierowej odpowiadają sekretarki, pielęgniarki oddziałowe/ koordynujące/ kierownicy komórek/pracowni oraz pielęgniarki poszczególnych Poradni.
6. Wszystkie skierowania na badania są przekazywane do Pracowni Medycznego Laboratorium Diagnostycznego (MLD) oraz Działu Diagnostyki Obrazowej (DDO)- w wersji papierowej.
7. W przypadku braku możliwości wydrukowania w Oddziale/ Poradni kodu na fiolki/ pojemniki z materiałem do badania, opisuje się ręcznie i niekodowane przekazuje do odpowiedniej Pracowni. Naklejanie kodów odbywa się w MLD.
8. W przypadku materiałów do badań dane do systemu ze skierowania wprowadza pracownik MLD, natomiast w przypadku badań radiologicznych dane ze skierowania wprowadza do systemu technik DDO.
9. Po usunięciu awarii/ zakończonej aktualizacji systemu informatycznego, należy niezwłocznie wprowadzić dane do systemu informatycznego na podstawie zapisów z dokumentacji papierowej.

10. W przypadku korzystania z dokumentacji papierowej, należy zapewnić odpowiednie zabezpieczenie dokumentów przed zagubieniem, uszkodzeniem lub nieautoryzowanym dostępem.

24. PRACA ZDALNA

24a. Praca zdalna wykonywana przez upoważnionych pracowników Szpitala

1. Upoważnieni przez AD pracownicy (w tym informatycy), mogą przetwarzać dane osobowe za pomocą zdalnego dostępu.
2. Wszystkie zdalne połączenia do sieci wewnętrznej Szpitala wymagają zgody AD.
3. W wyjątkowych przypadkach, jeśli uzyskanie zgody od AD jest niemożliwe, dopuszcza się połączenie zdalne z systemem, po uzyskaniu zgody ASI. Fakt ten łączący się informatyk zgłasza, najszybciej jak jest to możliwe AD.
4. Pracownik, w trakcie pracy zdalnej jest zobowiązany do przetwarzania danych w tym danych osobowych zgodnie z przepisami prawa, w szczególności z przepisami o ochronie danych osobowych oraz wewnętrznymi procedurami.
5. W ramach pracy zdalnej pracownik zobowiązany jest do przetwarzania udostępnionych mu danych jedynie w celach służbowych.
6. Wykonywanie pracy w formie zdalnej odbywa się na służbowym lub prywatnym sprzęcie komputerowym (za zgodą AD).
7. Prywatny sprzęt komputerowy wykorzystywany do pracy zdalnej jest obowiązkowo poddawany przeglądowi przez Zespół ds. informatycznych, który zweryfikuje, czy:
 - na urządzeniu jest legalne i aktualne oprogramowanie,
 - zostały włączone automatyczne aktualizacje,
 - została włączona zaporę systemową,
 - został zainstalowany i działa w tle program antywirusowy,
 - wyłączono autouzupełnianie i zapamiętywanie hasła w przeglądarce internetowej,
 - został zainstalowany program umożliwiający zaszyfrowanie i odszyfrowanie danych (np. 7-zip),
 - zostało ustawione automatyczne blokowanie urządzenia po dłuższym braku aktywności.
8. Logowanie do systemu operacyjnego wymaga potwierdzenia tożsamości użytkownika przez dwuskładnikowe uwierzytelnianie (2FA), np. sms na telefon komórkowy osoby łączącej się z siecią.
9. Pracownik jest odpowiedzialny za właściwe zabezpieczenie danych, przetwarzanych przez niego w ramach pracy zdalnej.
10. Pracownik zobowiązany jest do zachowania poufności informacji, w szczególności podczas służbowych rozmów telefonicznych lub wideokonferencji.
11. Pracownik zobowiązany jest do zabezpieczania dostępu do posiadanych danych służbowych przed osobami postronnymi, w tym wspólnie z nim zamieszkującymi oraz przed ich nieuprawnionym zniszczeniem lub modyfikacją.
12. Pracownik zobowiązany jest do uniemożliwienia wglądu osobom postronnym, w treści wyświetlane na ekranie komputera.
13. Pracownik zobowiązany jest do stosowania polityki czystego ekranu.
14. Pracownik zobowiązany jest po zakończeniu pracy każdorazowo wylogować się z programów oraz systemów wykorzystywanych do pracy zdalnej.
15. Sprzęt komputerowy powinien być podłączony do zabezpieczonej, domowej sieci LAN/WiFi.
16. Oprogramowanie urządzenia sieciowego powinno być regularnie aktualizowane.
17. Możliwość konfiguracji sprzętu sieciowego, który pracuje w wewnętrznej infrastrukturze teleinformatycznej z urządzeniami znajdującymi się poza siecią LAN, powinna być wyłączona lub ograniczona tylko do zdefiniowanych adresów IP.

18. Każda osoba posiadająca zdalny dostęp do zasobów teleinformatycznych Szpitala, zobowiązana jest przestrzegać zasad bezpieczeństwa oraz zgłaszać wszelkie stwierdzone fakty lub podejrzenia naruszenia bezpieczeństwa informacji.

19. W przypadku podejrzenia naruszenia zasad bezpieczeństwa zasobów teleinformatycznych należy zgłosić wystąpienie incydentu AD, bezpośredniemu przełożonemu, IOD lub ASI.

20. Logi z połączeń zdalnych są rejestrowane w systemie.

24b. Zdalny dostęp do zasobów sieci teleinformatycznej szpitala dla pracowników podmiotów zewnętrznych

1. Podmioty zewnętrzne, mogą otrzymać dostęp do systemów informatycznych Szpitala po podpisaniu umowy o powierzeniu przetwarzania danych osobowych.

25. REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

1. IOD prowadzi Rejestr czynności przetwarzania danych osobowych.

2. Rejestr czynności przetwarzania danych osobowych zawiera:

a) imię i nazwisko lub nazwę AD, dane kontaktowe IOD oraz współadministratorów danych;

b) cele przetwarzania;

c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;

d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;

e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej,

f) planowane terminy usunięcia poszczególnych kategorii danych;

g) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

3. Rejestr czynności przetwarzania danych osobowych zobowiązane są także prowadzić podmioty, którym szpital powierzył przetwarzanie danych osobowych.

26. REJESTR OCENY SKUTKÓW WPŁYWU NA PRYWATNOŚĆ (DPIA)

1. IOD w porozumieniu z ASI, przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

2. Nie dokonuje się oceny skutków, jeśli prawo reguluje daną operację. Jeżeli przetwarzanie reguluje daną operację przetwarzania lub zestaw operacji, a oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej.

3. Ocenę skutków dla ochrony danych, (jeżeli jest wymagana) prowadzi się zgodnie z wykazem rodzajów operacji przetwarzania.

4. Rejestr oceny skutków wpływu na prywatność powinien zawierać:

1) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania,

2) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów,

3) ocenę ryzyka naruszenia praw lub wolności osób fizycznych (pacjentów), których dane dotyczą,

4) środki planowane w celu minimalizacji ryzyka, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych zgodnie z RODO z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

27. ANALIZA RYZYKA

1. Niezależnie IOD i ASI (w odniesieniu do systemów i zasobów teleinformatycznych) przeprowadzają okresowe oceny ryzyka.
2. Analizę ryzyka przeprowadza się cyklicznie, minimum 1 raz w roku; a także niezwłocznie po każdym incydencie związanym z naruszeniem ochrony danych osobowych i cyberbezpieczeństwem.
3. Każdy pracownik ma obowiązek zgłaszania bezpośredniemu przełożonemu lub IOD, ryzyk zidentyfikowanych podczas wykonywania swoich obowiązków i przydzielonych zadań.
4. Zidentyfikowane ryzyko oraz ustalone metody jego ograniczenia są na bieżąco analizowane przez IOD i ASI.

§ 6

OPIS STRUKTURY ZBIORÓW DANYCH WSKAZUJĄCY ZAWARTOŚĆ POSZCZEGÓLNYCH PÓL INFORMACYJNYCH I WZAJEMNE POWIĄZANIA MIĘDZY NIMI

1. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi znajduje się w bazie danego systemu- stanowi **Załącznik nr 4** do **PBiIC**.

§ 7

POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH PODMIOTOM ZEWNĘTRZNYM

1. Szpital może powierzyć przetwarzanie danych innemu podmiotowi na podstawie umowy.
2. Umowa powierzenia przetwarzania danych powinna określać: przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą; prawa i obowiązki administratora oraz podmiotu przetwarzającego.
3. Umowy z podmiotami zewnętrznymi muszą zawierać postanowienia określające odpowiedzialność stron w obszarze bezpieczeństwa informacji i ciągłości działania.
4. Podmiot przetwarzający:
 - 1) przetwarza dane osobowe wyłącznie na udokumentowane polecenie AD,
 - 2) przestrzega zasad ochrony przetwarzania danych osobowych oraz zapisów umowy,
 - 3) podejmuje wszelkie niezbędne środki bezpieczeństwa dla ochrony przetwarzanych danych,
 - 4) może korzystać z usług innego podmiotu przetwarzającego, o ile AD wyraził pisemną zgodę na dalsze powierzenie,
 - 5) w miarę możliwości wspiera AD w zakresie wywiązywania się przez niego z obowiązków związanych z ochroną danych osobowych, nałożonych treścią rozporządzenia, a także udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia powyższych obowiązków,
 - 6) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie istniejące kopie, chyba że prawo nakazuje mu przechowywanie danych osobowych,
 - 7) umożliwia ADO, upoważnionemu pracownikowi lub audytorowi przeprowadzanie audytów, w tym inspekcji i kontroli.

Załącznik nr 1 do Zarządzenia nr 79 z dnia 16.06.2025 r.
POLITYKA BEZPIECZEŃSTWA INFORMACJI I CYBERBEZPIECZEŃSTWA
SZPITALA SPECJALISTYCZNEGO im. JĘDRZEJA ŚNIADECKIEGO
w NOWYM SĄCZU

5. Podmiot przetwarzający, może korzystać z usług innego podmiotu przetwarzającego, tylko po uzyskaniu zgody AD.
6. IOD prowadzi Rejestr umów powierzenia przetwarzania danych osobowych oraz użytkowników, którym nadano uprawnienia do zdalnego dostępu do sieci informatycznej szpitala.
7. Podmiot przetwarzający dane, zobligowany jest do stosowania środków technicznych i organizacyjnych, zapobiegających incydentom bezpieczeństwa informacji, nie niższy niż poziom zabezpieczenia danych w szpitalu.
8. Pracownicy podmiotów zewnętrznych podpisują stosowne upoważnienie i oświadczenie.
9. Podmiot zewnętrzny ponosi odpowiedzialność za skutki naruszeń bezpieczeństwa teleinformatycznego (w tym danych osobowych) przez swoich pracowników.
10. ASI/LAS/ Zespół ds. technicznych nadzorujący realizację umowy z podmiotem zewnętrznym wnioskuje do AD o nadanie upoważnień dla pracowników podmiotu zewnętrznego.
11. Upoważnienia do systemów informatycznych dla pracowników podmiotu zewnętrznego są przyznawane nie dłużej niż na czas trwania umowy.
12. ASI zawsze jest informowany o potrzebie zdalnego dostępu, każdorazowo wydaje na nie zgodę oraz nadzoruje wykonywane prace (lub wskazuje informatyka odpowiedzialnego za nadzór).
13. ASI prowadzi Rejestr zdalnych połączeń pracowników podmiotów zewnętrznych.
14. Zdalne połączenia są realizowane przez udostępnione przez Zespół ds. Informatycznych bezpieczne kanały.
15. Stacje robocze podmiotów zewnętrznych używane do zdalnego łączenia się zasobami teleinformatycznymi szpitala muszą być objęte w szczególności ochroną antywirusową i zabezpieczeniem dostępu sieciowego.

§ 8

WSPÓŁADMINISTROWANIE

1. Szpital może zawierać umowy o współadministrowanie danych z podmiotami zewnętrznymi.
2. W umowach o współadministrowanie należy określić: cel, okres umowy, sposoby przetwarzania oraz zakresy odpowiedzialności każdej strony dotyczące zachowania poufności danych.
3. Współadministrator, jest zobowiązany zapewnić wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, zgodnie z obowiązującymi przepisami, jak również:
 - do dołożenia należytej staranności przy przetwarzaniu powierzonych danych osobowych,
 - do zapewnienia zachowania w tajemnicy, przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji umowy, zarówno w trakcie zatrudnienia, jak i po jego ustaniu.
 - informowania o każdym naruszeniu ochrony danych osobowych lub incydentu bezpieczeństwa informacji bez zbędnej zwłoki,
4. Każdy ze współadministratorów przeprowadza analizę ryzyka w zakresie ochrony danych osobowych i cyberbezpieczeństwa.
5. Każdy ze współadministratorów, samodzielnie ponosi odpowiedzialność za skutki przetwarzania przez niego danych osobowych, w zakresie, w jakim każdy z nich przyczynił się do naruszenia obowiązujących zasad ochrony danych osobowych osoby fizycznej.
6. Współadministratorzy zobowiązani są do niezwłocznego informowania drugiej strony o każdym zdarzeniu, które mogłoby stanowić podstawę zgłoszenia roszczeń w związku z naruszeniem zasad

przetwarzania danych osobowych oraz incydentów dotyczących danych osobowych lub cyberbezpieczeństwa.

§ 9

UDOSTĘPNIANIE DANYCH OSOBOWYCH

1. Każda osoba ma prawo do dostępu do swoich danych (w tym do dokumentacji medycznej dotyczącej jego stanu zdrowia oraz udzielonych jej świadczeń zdrowotnych).
2. Udostępnienie danych osobowych następuje:
 - na wniosek osoby, której dane dotyczą lub osoby upoważnionej,
 - na podstawie przepisów prawa,
 - innemu administratorowi, jeżeli przetwarzanie jest niezbędne do zapewnienia ciągłości udzielania świadczeń zdrowotnych lub innych prawnie uzasadnionych celów.
3. Zasady udostępniania dokumentacji medycznej reguluje procedura „Udostępnianie i przechowywanie dokumentacji medycznej”, a zasady dot. udostępniania znajdują się we wszystkich komórkach organizacyjnych i na stronie internetowej Szpitala.

§ 10

ZARZĄDZANIE INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI I CYBERBEZPIECZEŃSTWEM

1. Za zgłoszenie incydentu w danej komórce organizacyjnej odpowiada każda osoba, która posiada taką informację.
2. Za zarządzanie incydentem, w tym usuwanie przyczyn incydentu odpowiada powołany Zespół ds. cyberbezpieczeństwa, który zapewnia obsługę incydentu w Szpitalu.
3. Za zgłaszanie incydentu niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT poziomu krajowego odpowiada IOD, a w przypadku jego nieobecności ASI/Koordinator Zespołu ds. informatycznych lub zastępujący informatyk.
4. Incydenty dotyczące bezpieczeństwa informacji obsługuje IOD.

1) Kategorie incydentów

1. Incydent bezpieczeństwa informacji oraz cyberbezpieczeństwa to zdarzenie, którego skutkiem jest lub może być naruszenie bezpieczeństwa aktywów informacyjnych oraz który powoduje lub może spowodować obniżenie, jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny. Jego przyczyną może być:
 - a) zdarzenie losowe zewnętrzne (np. klęski żywiołowe, pożary, zakłócenia w dostawie energii elektrycznej itp.), którego wystąpienie może spowodować zniszczenie lub uszkodzenie infrastruktury informatycznej albo dokumentacji papierowej oraz zakłócenie ciągłości pracy systemów nie powodując naruszenia poufności danych;
 - b) zdarzenie losowe wewnętrzne (np. błędy w oprogramowaniu, awarie sprzętu itp.), które mogą powodować zakłócenia ciągłości pracy systemów a także prowadzić do zniszczenia lub utraty danych;
 - c) świadome i celowe działania mające na celu naruszenie poufności zasobów informacyjnych, w tym poufności danych.

2) Incydentami bezpieczeństwa informacji w szczególności są:

- a) naruszenie poufności, to jest ujawnienie informacji niepowołanym osobom;

- b) naruszenie integralności, to jest zniszczenie, uszkodzenie lub przekłamanie informacji;
- c) naruszenie dostępności, to jest braku dostępu do danych przez uprawnionych użytkowników.

3) Przyczyny incydentów bezpieczeństwa informacji oraz cyberbezpieczeństwa mogą dotyczyć:

- a) niewłaściwego wykorzystywania zasobów informatycznych lub niewłaściwego postępowania z dokumentacją papierową;
- b) działania szkodliwego oprogramowania;
- c) prób omijania systemów zabezpieczeń;
- d) nieautoryzowanego dostępu do systemów, aplikacji i dokumentów;
- e) zniszczenia lub kradzieży urządzeń wykorzystywanych do przetwarzania i przechowywania informacji;
- f) zniszczenia lub kradzieży nośników danych;
- g) próby wyłudzeń informacji;
- h) ataków socjotechnicznych, ataków z wykorzystaniem technik zagrażających poufności, integralności lub dostępności informacji;
- i) naruszenia zasad obowiązujących w Szpitalu dotyczących bezpieczeństwa informacji, w tym danych osobowych.

4) Zgłaszanie incydentów związanych z bezpieczeństwem informacji oraz cyberbezpieczeństwem

1. W przypadku ujawnienia incydentu osoba niezwłocznie powiadamia o tym fakcie IOD - tel. (18) 44 25 722, email: abi@szpitalnowysacz.pl lub ASI, (gdy incydent dotyczy systemów informatycznych). Zgłoszenie następuje telefonicznie na nr tel. (18) 44 25 973 lub 795 531 805, e mail: asi@szpitalnowysacz.pl lub informatyka@szpitalnowysacz.pl

2. Telefoniczne zgłoszenie należy potwierdzić pisemną notatką służbową i przekazać IOD.

3. Notatka musi zawierać następujące informacje:

- a) imię i nazwisko osoby zgłaszającej;
- b) stanowisko oraz komórka organizacyjna, dane kontaktowe (e-mail, telefon);
- c) dokładne miejsce oraz datę wystąpienia incydentu;
- d) opis incydentu w sposób adekwatny do posiadanej wiedzy i umiejętności zgłaszającego (jakiego systemu dotyczy, opis incydentu, określenie wpływu incydentu na funkcjonowanie systemu, wstępne skutki i oszacowanie szkód.

4. Brak umiejętności poprawnego rozpoznania incydentu przez osobę zgłaszającą nie może być przyczyną zaniechania zgłoszenia.

5. W przypadku nieobecności IOD incydent należy zgłosić do ASI lub informatyka Zespołu ds. informatycznych. O incydencie osoba odbierająca zgłoszenie niezwłocznie informuje AD i IOD.

4a. Podejmowanie działań w związku ze zgłaszanymi incydentami naruszenia bezpieczeństwa przetwarzania danych osobowych.

1. W przypadku naruszenia ochrony danych osobowych mają zastosowanie przepisy art. 33-34 RODO.

2. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie ochrony danych osobowych tj.:

- a. przypadkowe lub niezgodne z prawem zniszczenie danych;
- b. przypadkowa lub niezgodna z prawem utrata danych;
- c. przypadkowa lub niezgodna z prawem modyfikacja danych;
- d. nieuprawnione ujawnienie danych;

Załącznik nr 1 do Zarządzenia nr 79 z dnia 16.06.2025 r.

**POLITYKA BEZPIECZEŃSTWA INFORMACJI I CYBERBEZPIECZEŃSTWA
SZPITALA SPECJALISTYCZNEGO im. JĘDRZEJA ŚNIADECKIEGO
w NOWYM SĄCZU**

e. nieuprawniony dostęp do danych osobowych; każdy pracownik zatrudniony przy przetwarzaniu danych osobowych (pracownik, stażysta, praktykant, itp.) jest zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie powiadomić o tym fakcie swojego bezpośredniego przełożonego oraz IOD i ASI (jeżeli naruszenie ma związek z systemami informatycznymi).

4. Fakt naruszenia lub podejrzenia naruszenia ochrony danych osobowych należy potwierdzić pisemnie poprzez niezwłoczne sporządzenie notatki służbowej, w której umieszcza się informację o dacie, czasie, miejscu, okolicznościach zdarzenia. Notatkę przekazuje się IOD. O zdarzeniu IOD niezwłocznie powiadamia AD.

5. W przypadku nieobecności IOD notatkę należy przekazać ASI.

6. Zgłoszenia są rejestrowane przez IOD w Rejestrze naruszeń i incydentów bezpieczeństwa informacji i cyberbezpieczeństwa.

7. Przy ocenie istotności incydentu pod uwagę brane są następujące czynniki:

- a) charakter naruszenia ochrony danych osobowych;
- b) kategorię i przybliżoną liczbę osób których dane dotyczą;
- c) kategorię i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
- d) możliwe konsekwencje naruszenia ochrony danych osobowych;
- e) wpływ incydentu na ciągłość działania;
- f) koszty usunięcia skutków incydentu;
- g) szacowany czas naprawy skutków wywołanych incydem.

8. Zakwalifikowanie zgłoszenia incydentu, jako „nieistotny” kończy postępowanie, o czym IOD informuje zgłaszającego.

9. Sprawdzenie naruszenia lub podejrzenia naruszenia ochrony danych osobowych kończy się sprawozdaniem, które przekazywane jest AD. Sprawozdania dokonuje IOD wraz z ASI.

10. W przypadku zakwalifikowania zdarzenia, jako naruszenie ochrony danych osobowych, które skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych, IOD za wiedzą AD bez zbędnej zwłoki, nie później niż w terminie 72 godzin od stwierdzenia naruszenia powiadamia Urząd Ochrony Danych Osobowych.

11. Zgłoszenia do UODO przekazywane są w sposób elektroniczny. Procedura zgłoszeń opisana jest pod adresem internetowym <https://uodo.gov.pl/pl/501/2278>

12. IOD wraz z ASI podejmuje również działania zabezpieczające i naprawcze zmierzające do minimalizacji skutków powstałych w wyniku incydentu, jak również działania zaradcze dla uniknięcia wystąpienia podobnych incydentów w przyszłości.

13. Jeżeli zawiadomienie osób, których dane dotyczą wymagałoby niewspółmiernie dużego wysiłku, IOD przygotowuje publiczny komunikat lub wybiera inny stosowny środek, za pomocą, którego zawiadomienie zostanie tym osobom przekazane.

14. W przypadku stwierdzenia działań zamierzonych, przy jednoczesnym zidentyfikowaniu sprawcy incydentu dotyczącego naruszenia bezpieczeństwa przetwarzania danych osobowych AD podejmuje decyzję dotyczącą wyciągnięcia ewentualnych konsekwencji dyscyplinarnych wobec sprawcy incydentu. Jednocześnie, w zależności od wagi incydentu, mogą być powiadomione organy ścigania.

4b. Podejmowanie działań w związku ze zgłaszaniem incydentami związanymi z cyberbezpieczeństwem

1. W przypadku incydentów związanych z cyberbezpieczeństwem, mają zastosowanie przepisy Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

2. Zgłoszenie incydentu rejestrowane jest przez IOD i jest niezwłocznie zgłaszane AD.

3. Osoba zgłaszająca incydent powinna w miarę możliwości zabezpieczyć materiał dowodowy (np. zrzut ekranu monitora, zdjęcie niezabezpieczonych materiałów zawierających dane osobowe itp.). Działania związane z obsługą zdarzenia w pierwszej kolejności dotyczą rozpoznania i kwalifikacji zgłoszenia. W przypadku, kiedy zgłoszenie zakwalifikowane zostało, jako incydent bezpieczeństwa informacji lub cyberbezpieczeństwa, dokonywana jest jego ocena istotności. Powyższe działania wykonuje IOD w porozumieniu z ASI oraz informatykami zatrudnionymi w Szpitalu, (jeżeli zgłoszenie dotyczy naruszenia cyberbezpieczeństwa).
4. Przy ocenie istotności incydentu pod uwagę brane są następujące czynniki:
 - a) powstałe szkody będące wynikiem incydentu;
 - b) wpływ incydentu na działanie systemów;
 - c) wpływ incydentu na ciągłość działania w Szpitalu;
 - d) koszty usunięcia skutków incydentu;
 - e) szacowany czas naprawy skutków wywołanych incydem;
 - f) oszacowanie zasobów koniecznych do przywrócenia ciągłości działania systemów.
5. Zakwalifikowanie zgłoszenia incydentu, jako „nieistotny” kończy postępowanie, o czym IOD informuje zgłaszającego i AD.
6. W przypadku zakwalifikowania zdarzenia, jako incydentu związanego z bezpieczeństwem informacji lub cyberbezpieczeństwem, Zespół odpowiedzialny za cyberbezpieczeństwo podejmuje działania zabezpieczające i naprawcze zmierzające do minimalizacji szkód powstałych w wyniku incydentu.
7. Komórki organizacyjne w miarę możliwości, są obowiązane także we własnym zakresie podjąć działania naprawcze, zmierzające do zniwelowania szkód powstałych w wyniku incydentu.
8. O wynikach analizy incydentu oraz podjętych działaniach naprawczych IOD informuje AD oraz zgłaszającego. W razie nieobecności IOD, zgłaszającego powiadamia ASI.
9. W przypadku stwierdzenia incydentu poważnego IOD (lub ASI w przypadku nieobecności IOD) nie później niż w ciągu 24 godzin od momentu wykrycia powiadamia AD i zgłasza incydent do właściwego CSIRT NASK (Naukowa i Akademicka Sieć Komputerowa - Państwowego Instytutu Badawczego ul. Kolska 12, 01- 045 Warszawa).
10. Zgłoszenia do CSIRT NASK przekazywane są w sposób elektroniczny. Procedura zgłoszeń opisana jest pod adresem internetowym <https://incydent.cert.pl/>
11. W przypadku braku możliwości przekazania go w sposób elektroniczny można zgłaszać przy użyciu innych dostępnych środków komunikacji (np. na numer telefonu +48 22 380 82 74 lub +48 22 380 82 00).
12. W zgłoszeniu przekazuje się informacje, zgodnie z formularzem oraz zgodnie z treścią art. 23 ust. 1 Ustawy o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r.
13. W przypadku stwierdzenia działań zamierzonych, przy jednoczesnym zidentyfikowaniu sprawcy incydentu dotyczącego naruszenia bezpieczeństwa informacji oraz cyberbezpieczeństwa AD podejmuje decyzję dotyczącą wyciągnięcia ewentualnych konsekwencji dyscyplinarnych wobec sprawcy incydentu. W zależności od wagi incydentu mogą być powiadomione organy ścigania.

§ 11

AUDYTY WEWNĘTRZNE I ZEWNĘTRZNE

1. Okresowe audyty wewnętrzne (przeprowadzane przez audytora wewnętrznego, auditorów wewnętrznych, IOD, ASI/LAS) i zewnętrzne (przeprowadzane przez auditorów zewnętrznych);

bezpieczeństwa informacji i cyberbezpieczeństwa są przeprowadzane zgodnie z obowiązującymi przepisami, normami i wytycznymi.

2. Każdy pracownik szpitala może zostać zobowiązany do przedstawienia informacji na temat przestrzegania procedur, wykorzystywania systemów informatycznych, zarządzania dostępem czy stosowania zasad ochrony danych osobowych.

3. Poddanie się audytowi jest obowiązkiem każdego pracownika oraz osób świadczących pracę na terenie Szpitala.

4. Audytowane osoby są zobowiązane do:

- zapewnienia dostępu do wymaganych zasobów, dokumentów oraz informacji,
- udzielania rzetelnych odpowiedzi na pytania audytorów,
- współpracy przy analizie i ocenie przestrzegania polityk bezpieczeństwa, procedur i standardów organizacji.

5. Zakres, przebieg i rezultaty audytów są dokumentowane i pisemnie przekazywane do AD.

§ 12

SZKOLENIA W ZAKRESIE OCHRONY DANYCH OSOBOWYCH

1. Każdy pracownik przetwarzający dane w Szpitalu jest zobowiązany do stałego podnoszenia wiedzy i kompetencji w zakresie ochrony danych.

2. Wszystkie osoby upoważnione do przetwarzania danych osobowych przed dopuszczeniem do przetwarzania muszą zostać przeszkolone w zakresie ochrony danych osobowych. Za przeprowadzenie szkolenia odpowiada IOD.

3. Szkolenie wstępne obejmuje m. in. zagadnienia dot.:

- 1) przepisów o ochronie danych osobowych,
- 2) zasad bezpiecznego użytkowania urządzeń i systemów informatycznych służących do przetwarzania danych osobowych,
- 3) zagrożeń na jakie może być narażone przetwarzanie danych osobowych, w szczególności związane z przetwarzaniem danych osobowych w systemach informatycznych,
- 4) zasad dostępu do pomieszczeń, w których przetwarzane są dane osobowe,
- 5) praw osób, których dane osobowe dotyczą,
- 6) sposobów postępowania w przypadku naruszenia ochrony danych osobowych lub systemu informatycznego,
- 7) odpowiedzialności z tytułu naruszenia ochrony danych osobowych.

4. Szkolenie w zakresie danych osobowych przeprowadza się każdorazowo po zaistnieniu zdarzenia zidentyfikowanego, jako incydent naruszenia ochrony danych osobowych, dla całego szpitala, grupy pracowników lub pracownika- w zależności od rodzaju incydentu.

5. Szkolenia są przeprowadzane cyklicznie przez IOD (min. 1 x na kwartał) oraz gdy zaistnieje taka potrzeba (w formie: szkolenie stacjonarne, przygotowanie prezentacji/materiałów, komunikaty w systemach informatycznych, wiadomości e-mail, itp.).

6. Pracownicy mają bieżący dostęp do aktualnej wersji dokumentów dot. ochrony danych i materiałów szkoleniowych na wydzielonej przestrzeni dyskowej w zasobach sieciowych szpitala (serwer Szpitala).

7. IOD oraz ASI regularnie podnoszą swoje kwalifikacje i wiedzę z zakresu cyberbezpieczeństwa: zagrożeń cybernetycznych, metod ochrony danych oraz obowiązujących przepisów prawnych

dotyczących bezpieczeństwa informacji (np. poprzez udział w dedykowanych OUK kursach, szkoleniach, konferencjach; szkoleniach zewnętrznych, itp.)

§ 13

PRZEGLĄDY I AKTUALIZACJE POLITYKI

1. **PBiC** podlega przeglądowi pod kątem aktualności co 2 lata.
2. Przeglądu i aktualizacji **PBiC** dokonuje IOD wraz z ASI.
3. Polityka podlega aktualizacji każdorazowo w przypadku:
 - wdrożenia nowego systemu informatycznego,
 - zmiany przepisów prawa dotyczących ochrony danych osobowych, wymagających aktualizacji **PBiC**,
 - innych znaczących zmian w funkcjonowaniu Szpitala mających wpływ na przetwarzanie danych osobowych,
 - stwierdzenia incydentów i naruszeń w zakresie świadczenia usług kluczowych i ochrony danych osobowych.

§ 14

POSTANOWIENIA KOŃCOWE

1. **PBiC** jest dokumentem wewnętrznym i nie może być udostępniania osobom nieuprawnionym.
2. Kierownicy komórek organizacyjnych są zobowiązani zapoznać podległy personel z treścią **PBiC**. Fakt zapoznania z **PBiC** pracownicy potwierdzają własnoręcznym podpisem.
3. Każda nowo zatrudniona osoba, upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem jej do przetwarzania danych z **PBiC** oraz podpisać stosowne oświadczenie.
4. Niezastosowanie się do wprowadzonej przez AD, **PBiC** i naruszenie procedur w zakresie ochrony danych i cyberbezpieczeństwa przez pracowników, może skutkować pociągnięciem do odpowiedzialności karnej na podstawie przepisów określonych w ustawie o ochronie danych osobowych oraz stanowi ciężkie naruszenie podstawowych obowiązków pracowniczych, które mogą być podstawą rozwiązania umowy o pracę w trybie art. 52 Kodeksu Pracy (postępowanie dyscyplinarne).
5. W sprawach nieuregulowanych w **PBiC** mają zastosowanie przepisy dotyczące ochrony danych osobowych oraz wydane na ich podstawie akty wykonawcze.
6. **PBiC** wchodzi w życie z dniem podpisania z mocą obowiązującą od dnia **1 lipca 2025 r.**

ZAŁĄCZNIKI:

Załącznik nr 1 Klasyfikacja i zasady postępowania z informacjami

Załącznik nr 2 Upoważnienie do przetwarzania danych osobowych

Załącznik nr 3 Oświadczenie

Załącznik nr 4 Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

Załącznik nr 1 do Zarządzenia nr 79 z dnia 16.06.2025 r.

**POLITYKA BEZPIECZEŃSTWA INFORMACJI I CYBERBEZPIECZEŃSTWA
SZPITALA SPECJALISTYCZNEGO im. JĘDRZEJA ŚNIADECKIEGO
w NOWYM SĄCZU**

Załącznik nr 1

***Klasyfikacja i zasady postępowania z informacjami przetwarzanymi w Szpitalu
Specjalistycznym im. Jędrzeja Śniadeckiego w Nowym Sączu***

Kategoria danych/ informacji	Opis	Przykładowe dokumenty	Oznaczenie	Wymagania organizacyjne	Zasady dostępu	Instrukcja postępowania	Zasady niszczenia
Publiczne (jawne)	Informacje nie muszą być zabezpieczone. Może o nich wiedzieć każdy, są ogólnodostępne: - nie zawierają danych osobowych - nie są prawnie chronione - nie zawierają tajemnic branżowych oraz ustawowo chronionych	ulotki , broszury, pisma informacyjne, instrukcje, zestawienia, raporty, materiały reklamowe	Do użytku publicznego	Oznacza właściciel dokumentu	Wobec tych dokumentów nie stosuje się ograniczeń	Brak zasad bezpieczeństwa	Brak
Wewnętrzne	Dane/ informacje przeznaczone do realizacji zadań służbowych przez pracowników na określonym stanowisku pracy, nie będące informacjami chronionymi.	Dokumenty wewnętrzne i inne informacje, które nie są przeznaczone dla osób nieuprawnionych. Regulaminy Polityki Instrukcje Procedury	Informacje wewnętrzne	Należy zabezpieczyć przed nieuprawnionymi osobami.	Wylącznie osoby uprawnione w zakresie niezbędnym do wykonywania obowiązków służbowych	Dokumenty mogą być wyносzone poza Szpital wyłącznie na służbowych laptopach lub na zaszyfrowanych nośnikach informacji. W przypadku wysyłania informacji partnerom i wykonawcom muszą być z nimi zawarte odpowiednie umowy. Dokumenty mogą być przesyłane przy użyciu wewnętrznej poczty e-mail z użyciem mechanizmów szyfrowania	Niszczarki lub w sposób uniemożliwiający odczyt. W przypadku danych elektronicznych ich usunięcie musi odbywać się w sposób uniemożliwiający ich odtworzenie.
Informacje chronione (tajemnica przedsiębiorstwa)	Informacje nieujawnione do publicznej wiadomości: informacje technologiczne i organizacyjne Szpitala, dane osobowe, wszystkie inne informacje posiadające wartość gospodarczą, które są chronione przez Szpital. Wymagają większych środków ochrony. Dostęp do tych informacji posiadają tylko osoby upoważnione, w związku z wykonywanymi czynnościami służbowymi.	Dokumenty zawierają dane osobowe chronione na podstawie RODO i Ustawy, zawierają tajemnice przedsiębiorstwa. Dokumentacja kadrowa, raporty z audytów, inne dokumenty i informacje istotne dla funkcjonowania Szpitala, informacje poufne i zastrzeżone.	Chronione (stanowiące tajemnicę Szpitala)	Za odpowiednie oznaczenie dokumentu oraz jego właściwe rozpowszechnianie odpowiedzialny jest właściciel dokumentu. Udostępnia on dokument jedynie osobom upoważnionym. Dokumenty są zabezpieczone, aby osoby nieuprawnione nie miały do nich dostępu.	Wylącznie osoby uprawnione w zakresie niezbędnym do wykonywania obowiązków służbowych	Dokumenty papierowe nie mogą być wyносzone poza Szpital bez zgody Dyrektora Szpitala. Jeżeli korzysta się z nośników elektronicznych to wymagane jest stosowanie mechanizmów szyfrujących Dyrektor autoryzuje przesyłanie informacji poza Szpital lub w jego imieniu robi to osoba przez niego upoważniona. Dokumenty mogą być przesyłane przy użyciu wewnętrznej poczty e-mail z użyciem mechanizmów szyfrowania. Dokumentacja kadrowo-płacowa powinna być szczególnie chroniona.	Dokumentacja papierowa podlega zniszczeniu za pomocą niszczarki, lub w sposób uniemożliwiający odczyt. W przypadku danych elektronicznych ich usunięcie musi odbywać się w sposób uniemożliwiający ich odtworzenie.
Informacje wrażliwe (wymagają najwyższych środków ochrony)	zgodnie z art. 9 RODO: - dane ujawniające pochodzenie rasowe lub etniczne, - dane ujawniające poglądy polityczne, - dane ujawniające przekonania religijne lub światopoglądowe, - dane ujawniające przynależność do związków zawodowych, - dane genetyczne, - dane biometryczne (wykorzystywane w celu jednoznacznego zidentyfikowania osoby fizycznej), - dane dotyczące zdrowia, - dane dotyczące seksualności lub orientacji seksualnej.	Dokumenty zawierają dane osobowe oraz dane szczególnych kategorii danych osobowych chronione na podstawie RODO i Ustawy	Informacje wrażliwe	Za odpowiednie oznaczenie dokumentu oraz jego właściwe rozpowszechnianie odpowiedzialny jest właściciel dokumentu. Udostępnia on dokument jedynie osobom upoważnionym. Dokumenty są zabezpieczone, aby osoby nieuprawnione nie miały do nich dostępu.	Wylącznie osoby uprawnione w zakresie niezbędnym do wykonywania obowiązków służbowych, na podstawie upoważnienia, zgodnie z zasadą wiedzy koniecznej do wykonywania czynności służbowych.	Dokumentacja medyczna, dostęp do informacji o Pacjentach i ich zdrowiu, jedynie przez osoby upoważnione	Dokumentacja papierowa podlega zniszczeniu za pomocą niszczarki, lub w sposób uniemożliwiający odczyt. W przypadku danych elektronicznych ich usunięcie musi odbywać się w sposób uniemożliwiający ich odtworzenie.

Załącznik nr 1 do Zarządzenia nr 79 z dnia 16.06.2025 r.
POLITYKA BEZPIECZEŃSTWA INFORMACJI I CYBERBEZPIECZEŃSTWA
SZPITALA SPECJALISTYCZNEGO im. JĘDRZEJA ŚNIADECKIEGO
w NOWYM SĄCZU

Załącznik nr 2

Aneks do zakresu czynności i obowiązków pracownika
Egz.

U P O W A Ż N I E N I E Nr

Na podstawie Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 679/2016 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) (Dz. U. UE L 119 z 4.05.2016 r., z późn. zm.) oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r., poz.1781 z późn. zm.),

Upoważniam Pana/Panią :

Forma zatrudnienia/ Stanowisko służbowe	Nazwa komórki organizacyjnej
Zatrudniony na podstawie:	Komórka organizacyjna – część medyczna:
Stanowisko:	Komórka organizacyjna– część administracyjna:
Od dnia:	Do dnia:

do przetwarzania danych osobowych znajdujących się w zakresie upoważnienia

Forma zbioru, system, moduł, schemat	Poziom dostępu						Symbol identyfikacji w systemie
	Odczyt (O)	Zapis (Z)	Modyfikacja (M)	Niszczenie / Usuwanie (N)	Powielanie / Druk (P)	Brak dostępu (B)	
1	2	3	4	5	6	7	8
PAPIEROWA w części:							
INFORMATYCZNA System: Moduł: Schemat:							

Nowy Sącz, dnia

.....
/podpis Administratora/

Egz. nr 1 – osoba upoważniona
Egz. nr 2 – akta osobowe

Otrzymał/a dnia

.....
/podpis osoby upoważnionej/

OŚWIADCZENIE

Oświadczam że, zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 679/2016 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), Dz. U. UE L 119 z 4.05.2016 r., z późn. zm.; oraz Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r., poz. 1781 z późn. zm.), **zobowiązuję się do zachowania w tajemnicy te dane osobowe oraz system ich zabezpieczenia, do których przetwarzania zostałam/em upoważniona/y.**

Zapoznałam/em się z Polityką Bezpieczeństwa Informacji i Cyberbezpieczeństwa Szpitala Specjalistycznego im. Jędrzeja Śniadeckiego w Nowym Sączu, oraz odpowiedzialnością cywilną i karną za nieuprawniony dostęp oraz przetwarzanie danych osobowych bez upoważnienia.

W czasie wykonywania swoich obowiązków służbowych zobowiązuję się do:

- Zapewnienia ochrony danych osobowych przetwarzanych w Szpitalu Specjalistycznym im. Jędrzeja Śniadeckiego w Nowym Sączu; zabezpieczenia przed udostępnieniem osobom nieuprawnionym, zabraniam, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem.**
- Zachowania w tajemnicy, także po ustaniu stosunku pracy, wszelkich informacji dotyczących funkcjonowania systemów lub urządzeń służących do przetwarzania danych osobowych oraz haseł dostępu do tych zbiorów.**

Zostałam/em poinformowany o odpowiedzialności karnej osoby upoważnionej do przetwarzania danych osobowych wynikającej z Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 679/2016 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), Dz. U. UE L 119 z 4.05.2016 r., z późn. zm.; oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r., poz. 1781 z późn. zm.):

Artykuł 82 Prawo do odszkodowania i odpowiedzialność- Rozporządzenia Parlamentu Europejskiego i Rady (UE):

„1. Każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę.

2. Każdy administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem naruszającym niniejsze rozporządzenie. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie, gdy nie dopełnił obowiązków, które niniejsze rozporządzenie nakłada bezpośrednio na podmioty przetwarzające, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom.

3. Administrator lub podmiot przetwarzający zostają zwolnieni z odpowiedzialności wynikającej z ust. 2, jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody.

4. Jeżeli w tym samym przetwarzaniu uczestniczy więcej niż jeden administrator lub podmiot przetwarzający lub uczestniczy w nim zarówno administrator jak i podmiot przetwarzający i zgodnie z ust. 2 i 3 odpowiadają za szkodę spowodowaną przetwarzaniem, ponoszą oni odpowiedzialność solidarną za całą szkodę, tak by zapewnić osobie, której dane dotyczą, rzeczywiste uzyskanie odszkodowania.

5. Administrator lub podmiot przetwarzający, który zgodnie z ust. 4 zapłacił odszkodowanie za całą wyrządzoną szkodę, ma prawo żądania od pozostałych administratorów lub podmiotów przetwarzających, którzy uczestniczyli w tym samym przetwarzaniu, zwrotu części odszkodowania odpowiadającej części szkody, za którą ponoszą odpowiedzialność, zgodnie z warunkami określonymi w ust. 2.

6. Postępowanie sądowe dotyczące odszkodowania jest wszczynane przed sądem właściwym na mocy prawa państwa członkowskiego, o którym mowa w art. 79 ust. 2”.

Art. 107- Ustawy o ochronie danych osobowych:

„1. Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności, albo pozbawienia wolności do lat dwóch.

2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej podlega grzywnie, karze ograniczenia wolności, albo pozbawienia wolności do lat trzech”.

Nowy Sącz, dnia

.....
/podpis osoby upoważnionej/

Egz. nr 1 – osoba upoważniona

Egz. nr 2 – akta osobowe

Załącznik nr 4
Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól
informacyjnych i powiązania między nimi

