Załącznik nr 1 do Zarządzenia Dyrektora ZOZ w Łowiczu nr 54 z dnia 15.09.2025r.

Polityka
bezpieczeństwa informacji
Zespołu Opieki Zdrowotnej w Łowiczu

Polityka ... 1
bezpieczeństwa informacji ... 1
Zespołu Opieki Zdrowotnej w Łowiczu ... 1
ROZDZIAŁ I ... 2
PRZEPISY OGÓLNE ... 2
ROZDZIAŁ II ... 4
ZASADY DOTYCZĄCE BEZPIECZEŃSTWA INFORMACJI ... 4
ROZDZIAŁ III ... 8
ODPOWIEDZIALNOŚĆ I UPRAWNIENIA W ZAKRESIE BEZPIECZEŃSTWA INFORMACJI ... 8
ROZDZIAŁ IV ... 10
KLASYFIKACJA INFORMACJI I ZASADY POSTĘPOWANIA Z INFORMACJAMI ... 10
ROZDZIAŁ V ... 12
DODATKOWE ŚRODKI OCHRONY INFORMACJI PRZETWARZANYCH W FORMIE ELEKTRONICZNEJ ... 12
ROZDZIAŁ VI ... 12
SZACOWANIE RYZYKA ... 12
ROZDZIAL VII ... 14
OGÓLNE ZASADY POSTĘPOWANIA Z INCYDENTAMI ... 14
ROZDZIAŁ VIII ... 14
POSTANOWIENIA KOŃCOWE ... 14

ROZDZIAŁ I

PRZEPISY OGÓLNE

§ 1. 1. Polityka bezpieczeństwa informacji, zwana dalej "Polityką", określa podstawowe zasady zarządzania bezpieczeństwem informacji oraz osoby odpowiedzialne za ochronę informacji w ZOZ.

2. Celem Polityki jest zapewnienie bezpieczeństwa informacji rozumianego jako zachowanie integralności i autentyczności, przed nieautoryzowaną zmianą oraz dostępności, rozliczalności i poufności.

3. Podstawę egzekwowania przestrzegania zasad niniejszej Polityki Bezpieczeństwa Informacji stanowią:

1) od pracowników - przepisy prawa oraz stosunek prawny będący podstawą wykonywania pracy na rzecz ZOZ,
2) od osób i podmiotów zewnętrznych - uczestniczących w procesach związanych z działalnością ZOZ przepisy prawa lub stosowne zapisy umów i porozumień,
3) użytkownicy przetwarzający szczególnie ważne informacje mogą być dodatkowo pisemnie zobowiązani do przestrzegania wyższych standardów.

§ 2. Użyte w Polityce pojęcia oznaczają:

4) informacja - wszelkie dane odnoszące się do osób do pomiotów lub procesów, niezależnie od ich formy i nośnika przetwarzania lub dystrybucji (ustne, pisemne, nagrania audio lub video), utrwalone na nośnikach elektronicznych, w systemach informatycznych, dokumentacji papierowej, będące własnością ZOZ lub udostępnione w ramach ofert, umów lub porozumień z osobami fizycznymi i podmiotami;
5) dostępność - właściwość polegająca na tym, że informacja jest dostępna na uprawnione żądanie;
6) integralność - właściwość polegająca na zapewnieniu dokładności i kompletności informacji;
7) poufność - właściwość polegająca na tym, że informacja może być udostępniana lub ujawniana wyłącznie w uzasadnionych przypadkach uprawnionym osobom lub podmiotom;
8) podatność - słabość lub wrażliwość, która może wpłynąć na wystąpienie zagrożenia i jego ewentualne skutki; może dotyczyć, w szczególności sposobu zarządzania lub postępowania, personelu, zależności, relacji, kontaktów wewnętrznych i zewnętrznych, czynnika technologicznego, niedoskonałości zabezpieczeń;
9) ryzyko - możliwość wykorzystania podatności przez zagrożenie, powodująca naruszenie bezpieczeństwa informacji;
10) incydent - zdarzenie które stwarza prawdopodobieństwo naruszenia bezpieczeństwa informacji lub zakłócenia realizacji zadań;

11) incydent poważny– incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi, straty finansowe lub wpływa na inne osoby fizyczne, osoby prawne, jednostki organizacyjnej nieposiadające osobowości prawnej poprzez wywołanie poważnej szkody materialnej lub niematerialnej w działaniu ZOZ;

12) SZBI - System Zarządzania Bezpieczeństwem Informacji, stanowiący część systemu zarządzania odnoszący się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji, obejmujący strukturę organizacyjną, polityki, planowane działania, odpowiedzialności, zasady, procedury, procesy i informacje;

13) użytkownik - pracownik, stażysta, wolontariusz, praktykant lub inna osoba wykonująca pracę bądź świadcząca usługi na podstawie umów cywilnoprawnych na rzecz ZOZ która uzyskała uprawnienie albo upoważnienie do przetwarzania informacji w określonym celu i zakresie, w tym do przetwarzania informacji w systemach teleinformatycznych;

14) osoba postronna - każda osoba, bez względu na jej związek z ZOZ, która nie jest uprawniona do przetwarzania danej informacji, lub na danym etapie;

15) przetwarzanie informacji - jakiekolwiek operacje przeprowadzane na informacjach, w ramach działalności ZOZ;

16) zabezpieczenie - działanie lub rozwiązanie, które ogranicza prawdopodobieństwo wystąpienia zagrożenia lub minimalizuje jego negatywne skutki; wyróżnia się trzy rodzaje zabezpieczeń funkcjonujących w ZOZ:

17) organizacyjne (struktury organizacyjne, polityki, procedury postępowania, zarządzenia, regulaminy, klauzule w umowach, zakresy obowiązków pracowników, szkolenia, audyty, kontrole itp.); techniczne (systemy bezpieczeństwa teleinformatycznego, systemy kontroli dostępu, urządzenia alarmowe, sygnalizacyjne lub monitoringu, oprogramowanie antywirusowe itp.); fizyczne (ogrodzenie, drzwi, zamykane szafy, sejfy, strefy ochronne itp.); środowiskowe (np. bezpieczeństwo okablowania, klimatyzacja);

18) zagrożenie - zdarzenie, zjawisko, działanie lub zaniechanie, które może skutkować incydentem albo doprowadzić do szkody lub nieosiągnięcia celów ZOZ.

§ 3. 1. Polityka jest podstawowym elementem w dokumentacji SZBI.

2. Polityką objęte są wszystkie informacje będące w dyspozycji ZOZ.

3. Zapisy Polityki należy uwzględniać w procesie opracowania pozostałej dokumentacji SZBI, w szczególności polityk, procedur, instrukcji i wytycznych obowiązujących w ZOZ.

4. Obowiązujące w ZOZ regulacje wewnętrzne należy opracowywać i wdrażać z uwzględnieniem założeń zapewniających ochronę informacji.

5. Jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ich ochronę, niż wynika to z Polityki, stosuje się przepisy tych ustaw.

§ 4. Polityka ma zastosowanie do wszystkich komórek organizacyjnych ZOZ i obejmuje zakresem obszar ZOZ, oraz miejsca i sytuacje, w których informacje ZOZ są przetwarzane poza jego siedzibą, w szczególności w kontekście zdalnego korzystania z sieci komputerowej ZOZ, w tym pracy zdalnej.

§ 5. 1. Do przestrzegania Polityki zobowiązani są wszyscy użytkownicy przetwarzający informacje ZOZ.

2. Za zapoznanie z Polityką osób, o których mowa w ust. 1, odpowiada w przypadku:

1) pracowników wykonujących obowiązki w dniu wejścia w życie Polityki - osoba kierująca pracą komórki organizacyjnej;
2) osób świadczących usługi lub korzystających z usług świadczonych przez ZOZ na podstawie umów cywilnoprawnych kierownik komórki organizacyjnej przygotowującej umowę;
3) nowo zatrudnianych pracowników, stażystów, wolontariuszy i praktykantów Kierownik Działu Spraw Pracowniczych;
4) dokumentowanie faktu określonego w ust. 2) pkt 1) i 2) pozostawia się do uznania osobie, które tego dokonuje.

ROZDZIAŁ II

ZASADY DOTYCZĄCE BEZPIECZEŃSTWA INFORMACJI

§ 6. 1. Polityka realizowana jest w ZOZ poprzez:

1) zapewnienie odpowiedniej organizacji procesów przetwarzania informacji;
2) użytkowników posiadających odpowiednią wiedzę, umiejętności i zaangażowanie adekwatne do powierzonych zadań;
3) ochronę fizyczną, techniczną i organizacyjną informacji przed dostępem osób nieupoważnionych, w szczególności przed nieuprawnionym wykorzystaniem, zaborem, uszkodzeniem, modyfikacją lub zniszczeniem;
4) zabezpieczenie systemów informatycznych eksploatowanych w ZOZ przed zagrożeniami;
5) zabezpieczenie informacji ZOZ przed ich uszkodzeniem lub zniszczeniem w wyniku pożaru, zalania, ataku terrorystycznego, katastrof naturalnych lub innych zagrożeń;
6) zapewnienie ciągłości działania procesów przetwarzania informacji w ZOZ;
7) zapewnienie możliwości sprawnego odtworzenia informacji w przypadku ich uszkodzenia;
8) zapewnienie gotowości do reakcji na incydenty i zagrożenia;
9) zapewnienie rozwiązań organizacyjnych i systemowych regulujących zasady i sposób zarządzania bezpieczeństwem informacji;
10) zapewnienie spójnej polityki informacyjnej ZOZ;

11) zapewnienie właściwych zapisów w zakresie bezpieczeństwa informacji, w szczególności stosowanie klauzul poufności; również po ustaniu współpracy w umowach o pracę a także umowach cywilnoprawnych z kontrahentami lub wykonawcami;

12) zapewnienie użytkownikom szkoleń z zakresu bezpieczeństwa informacji;

13) zapewnienie działań kontrolnych w zakresie przestrzegania zasad określonych w Polityce;

14) przestrzeganie zasad bezpieczeństwa informacji, o których mowa w §8;

15) stosowanie zabezpieczeń adekwatnych do wymogów prawnych oraz wyników audytów lub analiz ryzyka bezpieczeństwa informacji;

16) budynki i pomieszczenia, w których przetwarzane są dane osobowe, powinny być zabezpieczone w sposób uniemożliwiający dostęp do nich osobom postronnym, na czas nieobecności osób przetwarzających poprzez adekwatne rozwiązania techniczne.

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

3. w doborze zabezpieczeń należy kierować się w szczególności:

1) adekwatnością,

2) uwzględnieniem wyników szacowania ryzyka;

4. Należy unikać niepotrzebnego dublowania zabezpieczeń, przy uwzględnieniu racjonalnego gospodarowania środkami publicznymi, optymalizacji potrzeb oraz ograniczeń i uwarunkowań prawno-organizacyjnych ZOZ;

5. Za zagrożenia bezpieczeństwa informacji uważa się, w szczególności:

1) opuszczanie pomieszczenia bez jego zabezpieczenia, w ramach udostępnionych możliwości technicznych oraz bez odpowiedniego zabezpieczenia znajdujących się w nim informacji i środków służących do ich przetwarzania; pozostawiania drzwi do pomieszczenia niezamkniętych na klucz przez ostatnią wychodząca osobę, pozostawiania klucza w zamku od zewnątrz, zarówno podczas pobytu w pomieszczeniu jak również po opuszczeniu go i zamknięciu zamka;

2) brak nadzoru nad pomieszczeniem gdzie przetwarza się informacje mogący skutkować nieuprawnionym dostępem;

3) pozostawiania otwartych okien w pomieszczeniach, zwłaszcza na porterze; w razie konieczności, za wyjątkiem pierwszej kondygnacji, okna mogą na czas chwilowej nieobecności pozostać uchylone;

4) pozostawianie otwartych okien obsługowych w pomieszczeniach rejestracji na czas nieobecności użytkownika;

5) naruszenie lub próbę naruszenia integralności systemu przeznaczonego do przetwarzania informacji;

6) naruszenie lub próbę naruszenia integralności informacji w systemie przeznaczonym do ich przetwarzania - wszelkie modyfikacje (dodanie, zmiana, usuniecie), zniszczenie lub próby ich dokonania przez osoby nieuprawnione lub uprawnione działające w złej wierze

lub jako błąd osoby uprawnionej (np. zmiana treści danych, utrata całości lub części danych);

7) naruszenie poufności poprzez celowe lub przypadkowe wejście w posiadanie nadmiarowych informacji;

8) udostępnienie informacji osobie nieuprawnionej do ich otrzymania lub w nadmiarowym zakresie oraz narażenie na takie zdarzenie;

9) naruszenie ochrony informacji w systemie (np. nieautoryzowane logowanie do systemu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu);

10) nieuprawniony dostęp lub próbę dostępu do pomieszczenia, gdzie przetwarza się informacje;

11) ujawnienie indywidualnych haseł użytkowników lub innych danych dostępowych do systemu przetwarzającego informacje;

12) wykonanie nieuprawnionych kopii informacji;

13) zmiana lub usuniecie informacji zapisanych na kopiach bezpieczeństwa lub kopiach archiwalnych;

14) zamierzona lub przypadkowa utrata informacji źródłowych;

15) zamierzoną lub niezamierzoną utratę poufności danych poprzez utratę sprzętu mobilnego, klucza do podpisu elektronicznego, nośnika danych lub innego składnika systemu teleinformatycznego;

16) brak dostępności informacji w wymaganym czasie lub zakresie, w tym nośnika, wydruku, sprzętu;

17) brak dostępu uprawnionych osób do informacji, do których dostęp winien być zapewniony;

18) niewłaściwe niszczenie nośników informacji (np wydruków, pamięci zewnętrznych, płyt);

19) utratę oznaczonego klucza do pomieszczenia jeżeli nie można wykluczyć możliwości użycia go przez osobę postronną;

20) przebywanie osoby postronnej, bez nadzoru użytkownika, w pomieszczeniu gdzie przetwarzane są informacje lub spowodowanie takiego ryzyka.

§ 7. 1. Skuteczność SZBI zachowuje się przy jednoczesnym zastosowaniu i uzupełnianiu się elementów regulujących obszary bezpieczeństwa fizycznego, środowiskowego, technicznego i organizacyjnego.

2. Poziom bezpieczeństwa informacji jest odpowiedni wówczas, gdy spełnione są następujące warunki;

1) dokonano szacowania ryzyka w odniesieniu do bezpieczeństwa informacji;

2) wdrożono skuteczne zabezpieczenia wymagane przepisami prawa i Polityką.

§ 8. 1. W ZOZ stosuje się następujące zasady dotyczące bezpieczeństwa informacji:

1) wiedzy niezbędnej - użytkownicy posiadają dostęp tylko do tych informacji, które są konieczne do realizacji powierzonych im zadań; zabronione jest zarówno udostępnianie jak i wchodzenie w posiadanie informacji wykraczającej poza ten zakres; zasady nie stosuje się wobec informacji upublicznionych przez ZOZ;

2) indywidualnej odpowiedzialności - za utrzymanie odpowiedniego poziomu bezpieczeństwa poszczególnych informacji lub ich elementów odpowiadają określeni użytkownicy, w zakresie nałożonych obowiązków lub nadanych uprawnień;

3) niewygody uzasadnionej - bezpieczeństwo co do zasady opiera się na ograniczeniach oraz jest niewygodne; środki ochrony nie mogą nadmiernie utrudniać realizacji celów i zadań ZOZ;

4) czystego biurka i czystego ekranu - podczas dłuższej nieobecności pracownika na stanowisku pracy dokumenty i informatyczne nośniki danych, w miarę możliwości organizacyjno-technicznych, należy przechowywać w odpowiednio zabezpieczonych meblach biurowych lub szafach metalowych/sejfach;

5) ograniczonego zaufania - wszelkie informacje służbowe mogą być przekazywane wyłącznie w celu wykonywania zadań w zakresie do tego niezbędnym oraz osobom upoważnionym do pozyskania tych informacji; zasady nie stosuje się wobec informacji upublicznionych przez ZOZ;

6) obecności koniecznej - prawo przebywania w pomieszczeniach istotnych dla bezpieczeństwa informacji mogą mieć tylko wyznaczeni do tego użytkownicy; inne osoby nieuprawnione nie mogą zostać pozostawione w tych pomieszczeniach bez nadzoru; dostęp personelu technicznego zajmującego się konserwacją sprzętu, partnerów handlowych, pacjentów oraz innych osób do ww. pomieszczeń musi być nadzorowany;

7) zamykania pomieszczeń - niedopuszczalne jest pozostawienie pod nieobecność pracownika niezabezpieczonego pomieszczenia służbowego, zarówno w godzinach pracy, jak i po jej zakończeniu; na zakończenie dnia pracy ostatnia wychodząca z pomieszczenia osoba powinna zamknąć wszystkie okna i drzwi oraz zabezpieczyć klucze do pomieszczenia. Przed rozpoczęciem pracy należy się upewnić czy nie doszło do naruszenia zabezpieczenia pomieszczenia;

8) nadzorowania informacji - po godzinach pracy wszystkie nośniki informacji zawierające informacje podlegające ochronie powinny być przechowywane w miejscach zabezpieczonych przed dostępem osób nieuprawnionych;

9) stałej gotowości - niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających system funkcjonujący w ZOZ bez zastosowania alternatywnych mechanizmów; system powinien być sprawny i przygotowany na zidentyfikowane zagrożenia;

10) zgłaszania - każdy użytkownik ma obowiązek niezwłocznie zgłosić wystąpienie lub podejrzenie wystąpienia incydentu lub zagrożenia;

11) adekwatności zabezpieczeń - używane mechanizmy zabezpieczeń powinny być adekwatne do zagrożeń, podatności, wartości informacji oraz innych istotnych okoliczności;

12) kompleksowości ochrony - ochrona informacji powinna opierać się na stosowaniu różnych mechanizmów ochrony, w tym ochrony: prawnej, fizycznej, technicznej oraz organizacyjnej;

13) ochrony niezbędnej - minimalny wymagany poziom bezpieczeństwa informacji wynika z obowiązujących przepisów prawa; zastosowanie wyższych poziomów bezpieczeństwa informacji uzasadniają szczególne potrzeby ZOZ i wyniki szacowania ryzyka;

14) bezpiecznej współpracy z podmiotami zewnętrznymi - dokumenty regulujące współpracę powinny zawierać stosowne klauzule bezpieczeństwa, w tym o zachowaniu poufności, zasadach postępowania z pozyskaną informacją, niszczenia lub zwrotu dokumentacji po jej wykorzystaniu;

15) ewolucji - SZBI jest stale monitorowany i dostosowywany do zmieniających się warunków wewnętrznych i zewnętrznych;

16) podwyższonego poziomu ochrony zbiorów informacji - zbiór informacji powinien być bardziej chroniony niż poszczególne informacje, które się na niego składają;

17) czystego kosza - dokumenty papierowe oraz informatyczne nośniki danych, z wyjątkiem materiałów promocyjnych, marketingowych i innych publicznie dostępnych, powinny być niszczone w sposób uniemożliwiający ich odczytanie;

18) najwyższej staranności - w sytuacjach, które nie zostały unormowane w przepisach ogólnie obowiązujących, Polityce lub innych przepisach wewnętrznych zachowuje się najwyższą staranność aby zapewnić bezpieczeństwo informacji.

2. Katalog zasad, o których mowa w ust. 1 jest otwarty i może być rozszerzony lub uszczegółowiony w innych dokumentach stanowiących dokumentację SZBI.

ROZDZIAŁ III

ODPOWIEDZIALNOŚĆ I UPRAWNIENIA W ZAKRESIE BEZPIECZEŃSTWA INFORMACJI

§ 9. 1. Odpowiedzialność za bezpieczeństwo informacji ponoszą wszyscy użytkownicy w zakresie odpowiednim do nałożonych na nich obowiązków, posiadanych uprawnień lub zapisów określonych w umowach, porozumieniach i innych pisemnych formach współpracy.

2. Niezależnie od zakresu, o którym mowa w ust. 1, pracownicy są zobowiązani do przestrzegania obowiązku zachowania tajemnicy pracodawcy zgodnie z przepisami prawa pracy oraz tajemnicy określonej w ustawach branżowych.

3. Użytkownik, któremu przypisano odpowiedzialność za bezpieczeństwo informacji, może przekazywać swoje zadania innym użytkownikom, jednak pozostaje odpowiedzialny za bezpieczeństwo powierzonych informacji.

4. Użytkownik z uwzględnieniem możliwości technicznych i lokalowych podczas przetwarzania danych, podejmuje niezbędne środki w celu minimalizacji ryzyka naruszenia poufności danych.

§ 10. 1. Dyrektor ZOZ decyduje o celach i środkach przetwarzania informacji, w tym danych osobowych, jako ich administrator a w szczególności;

1) zarządza wprowadzenie szczególnych środków ochronnych dla newralgicznych elementów SZBI,
2) ustanawia SZBI oraz politykę;
3) akceptuje wyniki przeglądów zarządzania bezpieczeństwem informacji oraz raporty z incydentów bezpieczeństwa;
4) wydaje wewnętrzne akty normatywne regulujące zasady funkcjonowania i zarządzania bezpieczeństwem informacji;
5) określa kierownikom komórek organizacyjnych ZOZ zadania mające na celu zapewnienie bezpieczeństwa informacji, w przypadku wystąpienia takiej potrzeby;
6) egzekwuje odpowiedzialność użytkowników za naruszenia związane z bezpieczeństwem informacji, w zakresie adekwatnym do nałożonych na nich obowiązków i posiadanych uprawnień;
7) nadzoruje działania związane z usuwaniem zagrożeń, incydentów i incydentów poważnych:
8) przyjmuje wyjaśnienia od użytkowników, w szczególności w przypadku wystąpienia incydentów i zagrożeń w obszarze bezpieczeństwa informacji;
9) wyznacza lub powołuje: Inspektora Ochrony Danych, Pełnomocnika do spraw Ochrony Informacji Niejawnych, Administratora Systemu Informatycznego, których szczegółowe zadania określają przepisy odrębne.

2. Kierownicy komórek organizacyjnych odpowiadają za:

1) bezpieczeństwo powierzonych im aktywów informacyjnych;
2) bieżący przepływ informacji;
3) bieżące analizowanie zagrożeń i podejmowanie działań w celu uniknięcia incydentów;
4) zarządzanie przywracaniem prawidłowego stanu w podległej komórce, po wystąpieniu incydentu lub incydentu poważnego oraz informowanie Dyrektora;
5) wdrożenie i przestrzeganie przez podwładnych pracowników Polityki oraz innych regulacji w tym obszarze;
6) organizację pracy komórki zapewniającą ochronę informacji;
7) rekomendowania rozwiązań zwiększających skuteczność SZBI;
8) zapewnienie gotowości komórki do działania podczas trwania incydentów poważnych;
9) umożliwienie użytkownikom podnoszenia poziomu wiedzy z zakresu bezpieczeństwa informacji;
10) właściwy tryb zgłaszania, postępowania i dokumentowania incydentów, zgodnie z wewnętrznymi regulacjami w tym zakresie.

3. Użytkownik odpowiada w szczególności za:

1) przestrzeganie Polityki oraz innych regulacji;
2) zgłaszanie zagrożeń i incydentów przełożonemu lub innej wyznaczonej osobie:

3) zgłaszanie przełożonemu lub innej wyznaczonej osobie wszelkich zidentyfikowanych słabości SZBI;
4) ochronę informacji w zakresie swojego zakresu obowiązków;
5) niezwłoczne reagowanie w przypadku wystąpienia lub podejrzenia wystąpienia incydentu oraz postępowanie zgodnie z § 14. ust. 1, 2, 3 i wewnętrznymi regulacjami w tym zakresie;
6) zachowanie w tajemnicy informacji pozyskanych w ramach wykonywania obowiązków zawodowych w ZOZ również po ustaniu zatrudnienia lub współpracy.

ROZDZIAŁ IV

KLASYFIKACJA INFORMACJI I ZASADY POSTĘPOWANIA Z INFORMACJAMI

§ 11. 1. W ZOZ przyjmuje się następującą klasyfikację informacji oraz zasady postępowania:

Grupa informacji	Opis	Postępowanie
Informacja publiczna	Informacje, których obowiązek udostępniania wynika z przepisów prawa, w szczególności informacje publiczne w rozumieniu Ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej. Informacje udostępniane w szczególności na stronach internetowych ZOZ, lub uprawnione żądanie.	Przetwarzanie i przechowywanie w sposób gwarantujący zachowanie integralności i dostępności informacji. Udostępnianie na zasadach i w trybie przewidzianym przepisami prawa. Przechowywanie i niszczenie zgodnie z przepisami prawa oraz przepisami kancelaryjnymi.
Informacje niechronione	Wybrane fakty z działalności, informacje o wybranych grupach pracowników	Przetwarzanie i przechowywanie: w sposób gwarantujący integralność i dostępność. Udostępnianie stosownie do decyzji Dyrektora ZOZ Przechowywanie i niszczenie zgodnie z przepisami kancelaryjnymi.
Informacja prawnie chroniona	Informacje stanowiące dane osobowe podlegające ochronie na mocy przepisów o ochronie	Przetwarzanie i przechowywanie w sposób gwarantujący integralność dostępność, poufność i rozliczalność

	danych osobowych. Informacje chronione na mocy ustawy o ochronie informacji niejawnych (uregulowane odrębnymi przepisami). Inne informacje chronione z mocy prawa.	oraz inne atrybuty bezpieczeństwa, które są wymagane dla danej informacji chronionej na podstawie właściwej ustawy. Udostępnianie wyłącznie osobom i podmiotom uprawnionym, z zachowaniem integralności, poufności i rozliczalności oraz zgodnie z wymaganiami określonymi w przepisach Przechowywanie i niszczenie zgodnie z przepisami prawa oraz przepisami kancelaryjnymi.
Informacja wrażliwa	Informacje wewnętrzne ZOZ, wytworzone w ZOZ lub na jego rzecz, nie wchodzące w zakres informacji zaklasyfikowanych do pozostałych grup. Są to informacje dostępne wewnątrz ZOZ oraz przeznaczone do użytku wewnętrznego. informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą (tajemnica przedsiębiorstwa).	Przetwarzanie i przechowywanie w sposób gwarantujący integralność dostępność, i poufność. Udostępnianie wyłącznie osobom uprawnionym (użytkownikom ZOZ, osobom/użytkownikom podmiotów, z którymi ZOZ zawarł stosowne umowy), w sposób gwarantujący zachowanie integralności i dostępności informacji oraz zgodnie z wymaganiami określonymi w przepisach prawa lub zawartych przez ZOZ umowach. Udostępnianie wyłącznie za zgodą Dyrektora ZOZ. Niszczenie zgodnie z wymogami określonymi w przepisach prawa oraz Instrukcją kancelaryjną.

2. Wprowadzenie klasyfikacji informacji, o której mowa w ust. 1 nie powoduje konieczności specjalnego fizycznego oznaczania informacji lub jej nośnika, dokonuje się jedynie oznakowania literowo-cyfrowego zgodnie z Jednolitym Rzeczowym Wykazem Akt.

3. Sposób postępowania z informacjami na etapie ich bieżącego przetwarzania oraz po jego zakończeniu, określa Instrukcja Kancelaryjna Zespołu Opieki Zdrowotnej w Łowiczu oraz przepisy branżowe.

4. Zbędne kopie, wydruki, zapiski, nie będące dokumentem źródłowym, powinny być niszczone niezwłocznie po ich wykorzystaniu, poprzez fizyczne rozkawałkowanie nośnika

w sposób uniemożliwiający odtworzenie informacji, wycofywane z użycia nośniki elektronicznie powinny być zniszczone mechanicznie lub nadpisane.

5. Przechowywanie informacji po okresie ich bieżącego przetwarzania oraz niszczenie dokumentów źródłowych, po upływie okresu przechowywania, odbywa się na podstawie Instrukcji w sprawie organizacji i działania składnicy akt w Zespole Opieki Zdrowotnej w Łowiczu.

6. Nośniki informacji w miarę możliwości należy przechowywać w szafach zamykanych na klucz.

ROZDZIAŁ V

DODATKOWE ŚRODKI OCHRONY INFORMACJI PRZETWARZANYCH W FORMIE ELEKTRONICZNEJ

§ 12. 1. Szczegółowe zasady funkcjonowania i użytkowania systemu informatycznego określa dokumentacja użytkowa systemu informatycznego ZOZ w Łowiczu.

2. Użytkownik wykonujący czynności zawodowe przy użyciu systemu informatycznego zobowiązany jest do zapoznania się i przestrzegania dokumentacji o której mowa w ust. 1.
3. Urządzenia mobilne udostępnione przez pracodawcę stanowią część systemu informatycznego i podlegają ochronie również poza czasem pracy.
4. Korespondencja drogą elektroniczną może być prowadzona tylko przy użyciu poczty zakładowej. Użycie adresów publicznych dostawców jest dopuszczalne wyłącznie w przypadku sprawy nagłej i awarii poczty zakładowej.
5. Wydruki z systemu informatycznego oraz zapisane nośniki elektroniczne podlegają ochronie jak dokumentacja w formie papierowej.
6. Informacje przetwarzane wyłącznie w stacji roboczej lub urządzeniu mobilnym, w tym pliki i dokumenty oraz wiadomości tekstowe należy usuwać niezwłocznie po ich wykorzystaniu, chyba że ich dalsze przetwarzanie jest nakazane przepisami prawa.
7. Uprawnienia do systemu informatycznego dla użytkownika na określonym poziomie są nadawane stosownie do zakresu obowiązków w trybie określonym w dokumentacji o której mowa w ust.1

ROZDZIAŁ VI

SZACOWANIE RYZYKA

§ 13. 1. W obszarze bezpieczeństwa informacji identyfikacja i analiza ryzyka jest obligatoryjna i przeprowadza się ją cykliczne, nie rzadziej niż raz w roku.

2. Analiza ryzyka powinna być dodatkowo wykonana zgodnie z potrzebami, w szczególności przed opracowaniem dokumentacji bezpieczeństwa dla danego obszaru lub systemu oraz po wystąpieniu istotnych zmian w danym obszarze lub systemie lub po zaistnieniu incydentu.

3. Analizę ryzyka przeprowadza się w odniesieniu do poszczególnych aktywów informacyjnych, przy użyciu macierzy ryzyka, w postaci iloczynu wagi skutku i prawdopodobieństwa.

4. Skutek określa się jako sumę skutków w pięciostopniowej skali dla poufności, dostępności i integralności.

Skutki wystąpienia zagrożenia -S	Skala
Naruszone wszystkie atrybuty informacji	1
Naruszona dostępność i integralność	0,8
Naruszona poufność i dostępność lub integralność	0,6
Naruszona dostępność lub integralność	0,4
Naruszona tylko poufność	0,2

5. Poziom prawdopodobieństwa wywodzi się z częstości zdarzeń zaistniałych w przeszłości.

Prawdopodobieństwo wystąpienia ryzyka -P	Skala
Bardzo rzadko 1x3-5 lat lub rzadziej	1
Rzadko 1 x 3 lata	2
Umiarkowanie -1 x na rok	3
Często - 1 x na miesiąc	4
Bardzo często - 1 x na tydzień	5

6. Szacowanie ryzyka odbywa się według wzoru

R% = P x S x100 gdzie:

R – poziom wyliczanego ryzyka,

P – wartość przypisana prawdopodobieństwu materializacji zagrożenia

S - wartość przypisana wadze zagrożenia

7. Przyjmuje się następujące poziomy ryzyka:

1) krytyczne, należy niezwłocznie podjąć dodatkowe działania >50,
2) wysokie, należy podjąć dodatkowe działania >40,
3) średnie, należy monitorować i miarę możliwości podjąć dodatkowe działania >30,
4) małe, nie ma potrzeby podejmowania dodatkowych działań >20,
5) nieistotne <20.

ROZDZIAL VII

OGÓLNE ZASADY POSTĘPOWANIA Z INCYDENTAMI

§ 14. 1. W przypadku wystąpienia incydentu lub incydentu poważnego niezwłocznie podejmuje się działania mające na celu:

1) zapobieżenie rozprzestrzenianiu się incydentu,
2) zmniejszenie potencjalnych skutków,
3) przywrócenie prawidłowego stanu.

2. W miarę możliwości zabezpiecza się dowody.

3. Po przywróceniu prawidłowego stanu należy szczegółowo przeanalizować przyczyny wystąpienia i podjąć decyzję na temat dalszego postępowania z ryzykiem.

4. Zdarzenia związane z bezpieczeństwem informacji winny być rejestrowane.

5. Zgłaszanie zdarzeń organom państwowym regulują odrębne przepisy.

§ 15. W przypadku czasowej niedostępności systemu informatycznego ciągłość pracy w niezbędnym zakresie może być zachowana poprzez przetwarzanie informacji w dokumentacji papierowej. Informacje tak przetwarzane po ustaniu niedostępności są wprowadzane do systemu informatycznego.

§ 16. Szczegółowe zasady postępowania z incydentami zaistniałymi w systemie informatycznym określają inne przepisy.

ROZDZIAŁ VIII

POSTANOWIENIA KOŃCOWE

§ 17. Dokumentacja z zakresu bezpieczeństwa informacji, o której mowa w § 3 ust. 3, jest wprowadzana odrębnymi regulacjami.

§ 18. Naruszenie świadome bądź przypadkowe przez użytkownika przepisów prawa powszechnie obowiązującego lub innych postanowień w zakresie bezpieczeństwa informacji, do których przestrzegania się jest obowiązany, stanowi podstawę do odstąpienia przez ZOZ od umowy bez zachowania okresu wypowiedzenia i żądania pokrycia powstałej szkody lub zapłaty kary umownej, jeżeli nie stoją temu na przeszkodzie postanowienia zawartej umowy.