Załącznik do Zarządzenia Dyrektora ZOZ w Łowiczu nr 27/2021 z dnia 06.04.2021 r.

Polityka

bezpieczeństwa informacji

Zespołu Opieki Zdrowotnej w Łowiczu

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. Zasady zarządzania bezpieczeństwem informacji w ZOZ zostały opracowane zgodnie z obowiązującymi przepisami, w tym w szczególności:

1) rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (tj. Dz. Urz. UE L 119 z 04.05.2016, str. 1), zwanym dalej "RODO";
2) ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (tj. Dz. U. z 2019 r. poz. 1781);
3) ustawą z dnia 6 września 2001r. o dostępie do informacji publicznej (tj. Dz. U. z 2020, poz. 2176);
4) ustawą z dnia 25 lutego 2016r. o ponownym wykorzystywaniu informacji sektora publicznego (tj. Dz. U. z 2019r. poz. 1446);
5) ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (tj. Dz. U. z 2019r. poz. 742);
6) ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tj. Dz. U. z 2020r. poz. 1369 ze zm.);
7) ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tj. Dz. U. z 2020r. poz. 346 ze zm.);
8) rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tj. Dz. U. z 2017 r. poz. 2247);

§ 2. Użyte w Polityce pojęcia oznaczają:

1) 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;
2) dostępność - właściwość polegająca na tym, że informacja jest dostępna na uprawnione żądanie;
3) incydent - zdarzenie które stwarza prawdopodobieństwo naruszenia bezpieczeństwa informacji lub zakłócenia realizacji zadań;
4) integralność - właściwość polegająca na zapewnieniu dokładności i kompletności informacji;
5) 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;

6) poufność - właściwość polegająca na tym, że informacja może być udostępniana lub ujawniana wyłącznie w uzasadnionych przypadkach uprawnionym osobom lub podmiotom;
7) ryzyko - możliwość wykorzystania podatności przez zagrożenie, powodująca naruszenie bezpieczeństwa informacji;
8) sytuacja awaryjna - zdarzenie w obszarze bezpieczeństwa informacji, którego skutki powodują utratę ciągłości lub ograniczenia w działaniu ZOZ;
9) 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;
10) 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;
11) przetwarzanie informacji - jakiekolwiek operacje przeprowadzane na informacjach, w ramach działalności ZOZ;
12) zabezpieczenie - działanie lub rozwiązanie, które ogranicza prawdopodobieństwo wystąpienia zagrożenia lub minimalizuje jego negatywne skutki; wyróżnia się trzy rodzaje zabezpieczeń funkcjonujących w ZOZ:

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

13) zagrożenie - zdarzenie, zjawisko, działanie lub zaniechanie, które może skutkować incydentem lub sytuacją awaryjną 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 korzystający z informacji 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 kierownik 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, praktykantów i ekspertów Kierownik Działu Spraw Pracowniczych;
4) osoby, o których mowa w ust. 1, zobowiązane są do złożenia oświadczenia o zapoznaniu się z treścią Polityki.

ZASADY DOTYCZĄCE BEZPIECZEŃSTWA INFORMACJI

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

1) zapewnienie odpowiedniej organizacji procesów przetwarzania informacji;
2) pracowników 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, nieuprawnioną 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, zjawisk naturalnych lub innych zagrożeń;
6) zapewnienie ciągłości działania procesów przetwarzania informacji w ZOZ;
7) zapewnienie możliwości sprawnego odtworzenia informacji w przypadku ich naruszenia;
8) zapewnienie gotowości do reakcji na incydenty i sytuacje awaryjne;
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 pracownikom 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.

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;

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

§ 7. 1. Skuteczność SZBI zachowuje się przy jednoczesnym zastosowaniu i uzupełnianiu się elementów regulujących obszary bezpieczeństwa fizycznego i środowiskowego, technicznego, 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 - pracownicy 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 sie 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) separacji obowiązków - pojedyncze osoby nie mogą wykonywać krytycznych zadań w całości;
6) 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;
7) 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;
8) 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;
9) nadzorowania informacji - po godzinach pracy wszystkie nośniki informacji zawierające informacje podlegające ochronie powinny być przechowywane w miejscach zabezpieczonych przed dostępem osób nieuprawnionych;

10) 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;
11) zgłaszania incydentów i sytuacji awaryjnych - każdy użytkownik ma obowiązek niezwłocznie zgłosić wystąpienie lub podejrzenie wystąpienia incydentu lub sytuacji awaryjnej;
12) adekwatności zabezpieczeń - używane mechanizmy zabezpieczeń powinny być adekwatne do zagrożeń, podatności, wartości informacji oraz innych istotnych okoliczności;
13) kompleksowości ochrony - ochrona informacji powinna opierać się na stosowaniu różnych mechanizmów ochrony, w tym ochrony: prawnej, fizycznej, technicznej oraz organizacyjnej;
14) 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;
15) 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;
16) ewolucji - SZBI jest stale monitorowany i dostosowywany do zmieniających się warunków wewnętrznych i zewnętrznych;
17) podwyższonego poziomu ochrony zbiorów informacji - zbiór informacji powinien być bardziej chroniony niż poszczególne informacje, które się na niego składają;
18) 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;
19) 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.

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.

3. Użytkownik, któremu przypisano odpowiedzialność za bezpieczeństwo informacji, może przekazywać swoje zadania innym użytkownikom, jednak pozostaje odpowiedzialny za poprawność wykonania przekazanych działań.

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

1) ustanawia SZBI oraz politykę;
2) akceptuje wyniki przeglądów zarządzania bezpieczeństwem informacji oraz raporty z incydentów bezpieczeństwa;
3) wydaje wewnętrzne akty normatywne regulujące zasady funkcjonowania i zarządzania bezpieczeństwem informacji;
4) określa kierownikom komórek organizacyjnych ZOZ zadania mające na celu zapewnienie bezpieczeństwa informacji, w przypadku wystąpienia takiej potrzeby;
5) egzekwuje odpowiedzialność pracowników ZOZ za naruszenia związane z bezpieczeństwem informacji, w zakresie adekwatnym do nałożonych na nich obowiązków i posiadanych uprawnień;
6) nadzoruje działania związane z incydentami i sytuacjami awaryjnymi;
7) przyjmuje wyjaśnienia od pracowników ZOZ, w szczególności w przypadku wystąpienia incydentów i nieprawidłowości w zakresie funkcjonowania SZBI;
8) wyznacza lub powołuje:
   a) Inspektora Ochrony Danych,
   b) Pełnomocnika do spraw Ochrony Informacji Niejawnych,
   których szczegółowe zadania określają przepisy odrębne.

2. Kierownicy komórek organizacyjnych odpowiadają za:

1) bieżące analizowanie zagrożeń i podejmowanie działań w celu uniknięcia incydentów i sytuacji awaryjnych;
2) wdrożenie i przestrzeganie przez podwładnych pracowników Polityki oraz innych regulacji w tym obszarze;
3) organizację pracy komórki zapewniającą ochronę informacji;
4) rekomendowania rozwiązań zwiększających skuteczność SZBI;
5) zapewnienie gotowości komórki do działania w sytuacjach awaryjnych i kryzysowych;
6) umożliwienie pracownikom podnoszenia poziomu wiedzy z zakresu bezpieczeństwa informacji;
7) 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) ochronę informacji w zakresie swojej właściwości;
3) niezwłoczne reagowanie w przypadku wystąpienia lub podejrzenia wystąpienia incydentu lub sytuacji awaryjnej oraz postępowanie zgodnie z § 13. 1, 4, 5 i wewnętrznymi regulacjami w tym zakresie;
4) zachowanie w tajemnicy informacji pozyskanych w ramach wykonywania obowiązków zawodowych w ZOZ również po ustaniu zatrudnienia lub współpracy.

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	Przetwarzanie i przechowywanie w sposób gwarantujący zachowanie

	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.	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 danych osobowych. Informacje chronione na mocy ustawy o ochronie informacji niejawnych (uregulowane odrębnymi przepisami). Inne informacje chronione z mocy prawa.	Przetwarzanie i przechowywanie w sposób gwarantujący integralność dostępność, poufność i rozliczalność 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	Przetwarzanie i przechowywanie w sposób gwarantujący integralność dostępność, i poufność. Udostępnianie wyłącznie osobom uprawnionym (pracownikom ZOZ, osobom/pracownikom 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

	przedsiębiorstwa).	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 udokumentowanych, dokonuje się w nich jedynie odwzorowania literowo-cyfrowego zgodnie z Instrukcją kancelaryjną

SZACOWANIE RYZYKA

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

2. Identyfikacja i analiza ryzyka powinna być dodatkowo realizowana zgodnie z potrzebami, w szczególności przed opracowaniem dokumentacji bezpieczeństwa dla danego obszaru lub systemu oraz po wystąpieniu istotnych zmian w danym obszarze lub systemie.

3. Identyfikację i analizę ryzyka przeprowadza się w oparciu o dostępne metodyki.

4. Identyfikacja i analiza ryzyka powinna być udokumentowana.

POSTĘPOWANIE ZE ZDARZENIAMI

§ 13. 1. W przypadku wystąpienia incydentu lub sytuacji awaryjnej niezwłocznie podejmuje się działania mające na celu zapobieżenie rozprzestrzenianiu się zdarzenia, zmniejszenie potencjalnych skutków, przywrócenie prawidłowego stanu oraz w miarę możliwości zabezpiecza dowody.

2. Po przywróceniu prawidłowego stanu należy zdarzenie szczegółowo przeanalizować i podjąć decyzję na temat dalszego postępowania.

3. Zdarzenia związane z bezpieczeństwem informacji winny być rejestrowane.

4. Użytkownik ma obowiązek informowania wyznaczonych osób lub przełożonego o wystąpieniu sytuacji awaryjnej, incydentu oraz o wszelkich zidentyfikowanych słabościach SZBI.

5. O innych zdarzeniach należy poinformować kierownika właściwej komórki organizacyjnej.

6. Zgłaszanie zdarzeń organom państwowym regulują odrębne przepisy.

§ 14 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.

§ 15. Za naruszenie bezpieczeństwa informacji uważa się, w szczególności:

1) opuszczanie obszaru przetwarzania informacji bez jego odpowiedniego zabezpieczenia oraz bez odpowiedniego zabezpieczenia znajdujących się w nim informacji i środków służących do ich przetwarzania;
2) brak nadzoru nad pomieszczeniem gdzie przetwarza się informacje mogące skutkować nieuprawnionym dostępem;

a) naruszenie lub próbę naruszenia integralności systemu przeznaczonego do przetwarzania informacji;
b) naruszenie lub próbę naruszenia integralnością informacji w systemie przeznaczonym do ich przetwarzania - wszelkie modyfikacje (dodanie, zmiana, usuniecie), zniszczenie lub próby ich dokonania przez osoby nieuprawnione lub

uprawnione działające w zlej wierze lub jako błąd osoby uprawnionej (np. zmiana zawartości danych, utrata całości lub części danych);

c) naruszenie poufności poprzez celowe lub nieświadome poprzez wejście w posiadanie informacji lub przekazanie informacji osobie nieuprawnionej do ich otrzymania oraz narażenie na takie zdarzenie;

3) naruszenie ochrony informacji w systemie (np. nieautoryzowane logowanie do systemu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu);
4) nieuprawniony dostęp lub próbę dostępu do pomieszczenia, gdzie przetwarza się informacje;
5) ujawnienie indywidualnych haseł użytkowników lub innych danych dostępowych do systemu przetwarzającego informacje;
6) wykonanie nieuprawnionych kopii informacji;
7) zmiana lub usuniecie informacji zapisanych na kopiach bezpieczeństwa lub kopiach archiwalnych;
8) zamierzoną lub niezamierzoną utratę poufności danych poprzez utratę sprzętu mobilnego, klucza do podpisu elektronicznego, nośnika danych lub innego składnika systemu teleinformatycznego;
9) zamierzoną lub niezamierzoną utratę dostępności informacji w tym np. nośnika, wydruku, sprzętu;
10) brak dostępu uprawnionych osób do informacji, do których dostęp winien być zapewniony;
11) niewłaściwe niszczenie nośników informacji (np. wydruków, pamięci zewnętrznych, płyt).

POSTANOWIENIA KOŃCOWE

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

§ 17. Naruszenie świadome bądź przypadkowe przez użytkownika przepisów prawa powszechnie obowiązującego lub innych postanowień w zakresie bezpieczeństwa informacji, do których przestrzegania się zobowiązał, stanowi podstawę do odstąpienia przez ZOZ od umowy bez zachowania okresu wypowiedzenia i żądania pokrycia powstałej szkody lub zapłaty kary umownej, jeżeli taki obowiązek wynika z zawartej umowy.