Rozdział 1.

Wprowadzenie

Dokument „Polityka Bezpieczeństwa w zakresie ochrony danych osobowych w Wojewódzkim Szpitalu Psychiatrycznym w Andrychowie" – zwany dalej: „Polityką Bezpieczeństwa", opisuje reguły dotyczące procedur zapewnienia bezpieczeństwa danych osobowych zawartych w tradycyjnych i informatycznych systemach.

Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów wspomagających pracę w Wojewódzkim Szpitalu Psychiatrycznym.

Dokument zwraca uwagę na konsekwencje, jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

Odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi współczesnym systemom informatycznym.

Dokument wskazuje sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych i jest w szczególności przeznaczony dla osób pracujących przy przetwarzaniu danych osobowych Wojewódzkim Szpitalu Psychiatrycznym w Andrychowie.

Niniejszy dokument został opracowany zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016r. *w sprawie ochrony osób fizycznych oraz rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. 2004.100.1024)*.

Polityka stanowi jeden ze środków organizacyjnych, mających na celu wskazanie, że przetwarzanie danych osobowych odbywa się zgodnie z tym rozporządzeniem, a także usprawnienie i usystematyzowanie organizacji pracy Administratora.

1.1. Informacje ogólne

Polityka bezpieczeństwa jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora z poszanowaniem obowiązujących w tym zakresie przepisów prawa, a w szczególności:

1. *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),*
2. przepisów ustawy z dnia 26 czerwca 1974r. *Kodeks pracy ((T.j. Dz. U. z 2020 r. poz. 1320; zm.: Dz. U. z 2018 r. poz. 2432, z 2021 r. poz. 1162 oraz z 2022 r. poz. 655.) oraz przepisów wykonawczych z nim związanych*,
3. przepisów ustawy z dnia 15 kwietnia 2011r. *o działalności leczniczej (Dz.U.2022.0.633) oraz przepisów wykonawczych z nią związanych,*
4. przepisów ustawy z dnia 19 sierpnia 1994r. *o ochronie zdrowia psychicznego (Dz.U.2020.0.685) oraz przepisów wykonawczych z nią związanych*,
5. przepisów ustawy z dnia 26 października 1982r. *o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi (Dz.U.2021.0.1119) oraz przepisów wykonawczych z nią związanych,*
6. przepisów ustawy z dnia 29 lipca 2005r. *o przeciwdziałaniu narkomanii (Dz.U.2020.0.2050) oraz przepisów wykonawczych z nią związanych,*
7. przepisów ustawy z dnia 5 grudnia 1996r. *o zawodach lekarza i lekarza dentysty (Dz.U.1921.0.790) oraz przepisów wykonawczych z nią związanych,*

8. przepisów ustawy z dnia 5 lipca 1996r. *o zawodach pielęgniarki i położnej (Dz.U.2022.0.551) oraz przepisów wykonawczych z nią związanych,*
9. przepisów ustawy z dnia 6 listopada 2008r. *o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U.2020.0.849) oraz przepisów wykonawczych z nią związanych,*
10. przepisów ustawy z dnia 5 grudnia 2008r. *o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi (Dz.U.2021.0.2069) oraz przepisów wykonawczych z nią związanych,*
11. przepisów ustawy z dnia 27 sierpnia 2004r. *o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz.U.2021.0.1285) oraz przepisów wykonawczych z nią związanych,*
12. przepisów ustawy z dnia 22 maja 2003r. *o działalności ubezpieczeniowej (Dz.U.2021.0.1130) oraz przepisów wykonawczych z nią związanych,*
13. Rozporządzeniem Ministra Zdrowia z dnia 9 listopada 2015r. *w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U.2020.0.666),*
14. oraz innych przepisów ustaw i rozporządzeń normujących przetwarzanie danych osobowych określonych kategorii.

Pod szczególną ochroną Wojewódzkiego Szpitala Psychiatrycznego w Andrychowie pozostają dane osobowe wymienione w Rozporządzeniu zwanym 2016/679 art. 9 ust 1 pkt.

Przetwarzanie danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym dopuszczalne jest tylko w związku z realizacją celów statutowych Szpitala i w granicach wynikających z przepisów Rozporządzenia 2016/679 art. 9 ust 2 pkt h.

Realizacja postanowień tego dokumentu ma zapewnić:

- ochronę danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów o ochronie danych osobowych, zmianą, utratą, uszkodzeniem lub zniszczeniem,
- właściwą ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa danych oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa przetwarzanych danych.

Odpowiedzialność za ochronę danych osobowych ponoszą wszyscy pracownicy Szpitala mający dostęp do danych w ramach swych obowiązków służbowych.

Obowiązkiem osób zatrudnionych przy przetwarzaniu danych osobowych jest przestrzeganie postanowień niniejszej Polityki bezpieczeństwa.

Integralną częścią Polityki Bezpieczeństwa są:

- *Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Wojewódzkim Szpitalu Psychiatrycznym w Andrychowie,*
- *Instrukcja postępowania w sytuacji naruszenia systemu ochrony danych osobowych,*

1.2. Definicje

Administrator (danych) - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. W ramach niniejszego dokumentu jest to Dyrektor Wojewódzkiego Szpitala Psychiatrycznego z siedzibą w Andrychowie.

RODO – rozporządzenie parlamentu europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z 27.04.2016 r. (Dz. Urz. UE L 119 z 4.05.2016 r.).

Dane osobowe – to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną przez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Przetwarzanie danych osobowych to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych i obejmuje zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych.

Podmiotem danych jest każda osoba fizyczna, która jest przedmiotem przetwarzanych danych.

Odbiorca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

Użytkownik – użytkownik systemu, osoba wykorzystująca sprzęt i oprogramowanie systemu do wykonywania zadań służbowych.

Ograniczenie przetwarzania - polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania

Inspektor Ochrony Danych (IOD) - to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi/podmiotowi przetwarzającemu /pracownikom w zakresie obowiązującego prawa o ochronie danych i tej polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego.

System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,

Zabezpieczenie danych w systemie informatycznym – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,

Usuwanie danych – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,

Naruszenie ochrony danych osobowych - jest to przypadkowy lub niezgodny z prawem incydent prowadzący do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

1.3. Ewidencja zasobów

W Wojewódzkim Szpitalu Psychiatrycznym Politykę Bezpieczeństwa stosuje się przede wszystkim do:

1. Danych osobowych przetwarzanych w systemach informatycznych.
2. Wszystkich informacji dotyczących danych pacjentów.
3. Wszystkich informacji dotyczących danych pracowników, w tym danych osobowych pracowników treści zawieranych umów o pracę.
4. Wszystkich danych kandydatów do pracy zbieranych na etapie rekrutacji.
5. Informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych.
6. Rejestru osób dopuszczonych do przetwarzania danych osobowych.
7. Innych dokumentów zawierających dane osobowe.

Informacje te są przetwarzane i składowane są zarówno w postaci dokumentacji:

- tradycyjnych, w szczególności w dokumentacji medycznej, kartotekach, księgach, raportach, rejestrach, skorowidzach, wykazach i w innych zbiorach ewidencyjnych;
- w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych funkcjonującym w budynku przy ul. Dąbrowskiego 19 w Andrychowie.

Polityka Bezpieczeństwa zawiera dokumenty dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

Zakresy ochrony danych osobowych określone przez dokumenty Polityki Bezpieczeństwa mają zastosowanie do systemów informatycznych, w których są przetwarzane dane osobowe, a w szczególności do:

- wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie;

- wszystkich lokalizacji - budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie;

- wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, stażystów i innych osób mających dostęp do informacji podlegających ochronie, w tym do członków zarządu nazwa podmiotu WSP.

Do stosowania zasad określonych przez dokumenty Polityki Bezpieczeństwa zobowiązani są wszyscy pracownicy w rozumieniu Kodeksu Pracy, stażyści oraz inne osoby mające dostęp do informacji podlegających ochronie, w tym członkowie zarządu.

Informacje niejawne nie są objęte zakresem niniejszej Polityki Bezpieczeństwa.

Filarami ochrony danych osobowych w Szpitalu są:

- legalność - jednostka realizuje poprzez dbałość o ochronę prywatności i przetwarza dane zgodnie z prawem
- bezpieczeństwo - jednostka zapewnia odpowiedni poziom bezpieczeństwa danych.
- prawa Jednostki czyli umożliwienie osobom, których dane są przetwarzane przez jednostkę wykonywanie swoich praw i prawa te realizuje.
- rozliczalność - wykonuje jednostka poprzez dokumentowanie sposobu spełnienia obowiązków związanych z ochroną danych w taki sposób by w każdej chwili móc wykazać zgodność z przepisami.

Szpital przetwarza dane osobowe z ogólnymi zasadami przetwarzania danych osobowych określonymi w art.5 RODO z poszanowaniem następujących zasad :

- zgodnie z prawem, w oparciu o co najmniej jedną przesłankę legalności przetwarzania danych osobowych wskazaną w art. 6 lub 9 RODO (*zasada legalności*),
- w sposób rzetelny przy uwzględnieniu interesów i rozsądnych oczekiwań osób, których dane dotyczą (*zasada rzetelności*),
- w sposób przejrzysty dla osób, których dane dotyczą (*zasada przejrzystości*),
- w konkretnych, wyraźnych i prawnie uzasadnionych celach (*zasada ograniczenia celu*),
- w zakresie adekwatnym, stosownym oraz niezbędnym dla celów, w których są przetwarzane (*zasada minimalizacji danych*),
- przy uwzględnieniu ich prawidłowości i ewentualnego uaktualniania (*zasada prawidłowości*),
- przez okres nie dłuższy, niż jest to niezbędne dla celów, w których są przetwarzane (*zasada ograniczenia przechowywania*),
- w sposób zapewniający odpowiednie bezpieczeństwo (*integralność i poufność*) w tym przeprowadza analizy ryzyka dla czynności przetwarzania danych, analizę ryzyka kategorii danych, ocenę skutków dla wysokiego ryzyka naruszenia praw, dostosowuje środki ochrony danych do ustalonego ryzyka, posiada procedury zarządzania incydentami.

Zakres przetwarzania danych osobowych

1. Administrator prowadzi:
- rejestr czynności przetwarzania danych osobowych, których jest administratorem,
- rejestr kategorii czynności przetwarzania dokonywanych w imieniu administratorów, którzy powierzyli mu przetwarzanie danych.

2. Rejestr, o którym mowa w pkt 1 zawiera, co najmniej następujące informacje:
- nazwę oraz dane kontaktowe Administratora Danych oraz wszelkich współadministratorów,
- gdy ma to zastosowanie imię, nazwisko lub nazwę oraz dane kontaktowe swojego przedstawiciela,
- imię i nazwisko oraz dane kontaktowe IOD,
- cele przetwarzania,
- opis kategorii osób, których dane dotyczą,
- opis kategorii danych osobowych,
- kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,
- gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,
- jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
- ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

3. Rejestr, o którym mowa w pkt 2 zawiera, co najmniej następujące informacje:
- nazwę oraz dane kontaktowe Administratora,
- imię i nazwisko lub nazwę oraz dane kontaktowe każdego administratora, w imieniu którego działa Administrator,
- gdy ma to zastosowanie, imię, nazwisko lub nazwę oraz dane kontaktowe przedstawiciela każdego administratora, w imieniu którego działa Administrator,
- gdy ma to zastosowanie, imię i nazwisko oraz dane kontaktowe IOD każdego administratora, w imieniu którego działa Administrator,
- kategorie przetwarzań dokonywanych w imieniu każdego z administratorów,
- gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,

- ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

4. Administrator prowadzi rejestry, o których mowa w pkt 1 w formie elektronicznej.
5. W przypadku zgłoszenia przez organ nadzoru żądania w tym zakresie, Administrator udostępnia mu prowadzone przez siebie rejestry.

Rozdział 2.

Katalog zagrożeń i incydentów naruszających ochronę danych osobowych

1. Rodzaje zagrożeń naruszających ochronę danych osobowych:

- zagrożenia losowe:
  - zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu) - ich wystąpienie może prowadzić do utraty integralności danych lub ich zniszczenia lub uszkodzenia infrastruktury technicznej systemu; ciągłość systemu zostaje zakłócona, jednak nie dochodzi do naruszenia poufności danych,
  - wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania) – w wyniku ich wystąpienia może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych,
- zagrożenia zamierzone (świadome i celowe naruszenie poufności danych) – w wyniku ich wystąpienia zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości - w ramach tej kategorii zagrożeń wyróżnia się:
  - nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
  - nieuprawniony dostęp do systemu z jego wnętrza,
  - nieuprawniony przekaz danych,
  - bezpośrednie zagrożenie materialnych składników systemu (np. kradzież sprzętu).

2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to w szczególności:

- sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu (np. wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne)
- niewłaściwe parametry środowiska (np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elekromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych),
- awarie sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych,
- pojawienie się odpowiedniego komunikatu alarmowego od części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
- pogorszenie się jakości danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenie systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
- naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
- modyfikacja danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia,
- niedopuszczalna manipulacja danymi osobowymi w systemie,
- ujawnienie osobom nieuprawnionym danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń,
- praca w systemie informatycznym, wskazująca nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych (np. praca przy komputerze osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnały o uporczywym nieautoryzowanym logowaniu),
- podmienienie albo zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub skasowanie bądź skopiowanie w sposób niedozwolony danych osobowych,

- rażące naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce lub kserokopiarce, nie zamknięcie pomieszczenia w którym przetwarzane są dane osobowe, nie wykonanie w określonym terminie kopii zapasowych, praca na danych osobowych w celach prywatnych itd.).

Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych, znajdujących się na dyskach, pendrive, płytach CD, DVD, taśmach magnetycznych, kartach pamięci oraz wydrukach komputerowych, w formie niezabezpieczonej (otwarte szafy, biurka, regały urządzenia archiwalne, brak szyfrowania danych i inne).

Rozdział 3.

Zakres informacji objętych polityką bezpieczeństwa oraz zakres zastosowania

Dokument Polityki Bezpieczeństwa opisuje zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem. Jest to zestaw praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych. Polityka Bezpieczeństwa, odnosi się całościowo do problemu zabezpieczenia danych osobowych tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie, jak i danych przetwarzanych w systemach informatycznych.

Na Politykę Bezpieczeństwa składają się następujące informacje:

1. Wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe,
2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
3. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,
4. Sposób przepływu danych pomiędzy poszczególnymi systemami,
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

W ramach zabezpieczenia danych osobowych ochronie podlegają:

1. Sprzęt komputerowy – serwer,
2. Oprogramowanie – kody źródłowe, programy użytkowe, systemy operacyjne, narzędzia wspomagające
   i programy komunikacyjne,
3. Dane zapisane na dyskach, dyskietkach, pendrive, płytach CD, DVD, kartach pamięci oraz dane podlegające przetwarzaniu w systemie,
4. Hasła użytkowników,
5. Bazy danych, kopie zapasowe i archiwa,
6. Dokumentacja – zawierająca dane systemu, opisująca jego zastosowanie, przetwarzane informacje itp.,
7. Wydruki, dokumentacja papierowa, z której dane są wprowadzane do systemu informatycznego.

3.1. Wykaz pomieszczeń tworzących obszar przetwarzania danych osobowych

1. Obszar przetwarzania danych osobowych w Wojewódzkim Szpitalu Psychiatrycznym w Andrychowie stanowi większość pomieszczeń w budynku Szpitala.
2. Ze względu na szczególne nagromadzenie danych osobowych szczególnej ochronie podlegają pomieszczenia ujęte w wykazie pomieszczeń tworzących obszar przetwarzania danych osobowych stanowiącym ***załącznik nr 1*** do niniejszej Polityki bezpieczeństwa.

3. W pomieszczeniach tworzących obszar, w którym przetwarzane są dane osobowe mają prawo przebywać wyłącznie osoby upoważnione do dostępu i/lub przetwarzania danych osobowych oraz osoby sprawujące nadzór i kontrole nad bezpieczeństwem przetwarzania tych danych.
4. Przebywanie osób nieuprawnionych w obszarach, gdzie przetwarzane są dane osobowe jest możliwy wyłącznie za zgodą Administratora danych i w obecności osoby upoważnionej do przetwarzania danych osobowych.
5. Pomieszczenia, w których są przetwarzane dane osobowe, muszą być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych osobowych w taki sposób, aby uniemożliwić dostęp do nich osób nieuprawnionych.
6. W pomieszczeniach, w których przebywają osoby postronne, monitory komputerów powinny być ustawione w taki sposób, aby uniemożliwić im wgląd w dane osobowe.

3.2. Wykaz zbiorów danych osobowych i programów zastosowanych do przetwarzania danych

1. Wojewódzki Szpital Psychiatryczny w Andrychowie realizując Politykę bezpieczeństwa w zakresie ochrony danych osobowych sprawuje nadzór nad rodzajami oraz zawartością zbiorów danych osobowych.
2. Wykaz zbiorów danych osobowych i programów zastosowanych do ich przetwarzania zawarty jest w ***załączniku nr 2*** do niniejszej Polityki bezpieczeństwa.
3. Zabrania się tworzenia zbiorów danych osobowych, a także gromadzenia w zbiorach lub poza nimi kategorii danych osobowych innych niż jest to niezbędne dla realizacji celów statutowych Szpitala.
4. Do przetwarzania danych w zbiorach papierowych oraz w systemach informatycznych nadawane są upoważnienia. Za ich nadawanie / anulowanie odpowiada Administrator.
5. Upoważnienia mogą być nadawane w formie poleceń, np. upoważnienia do przeprowadzenia kontroli, wykonania czynności służbowych, udokumentowanego polecenia Administratora w postaci umowy powierzenia
6. Inspektor Ochrony Danych prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych. Wykaz ewidencji osób upoważnionych jest dokumentem wewnętrznym, natomiast wzór takiej ewidencji stanowi ***załącznik nr.3.***
7. Wzór upoważnienia zawarty jest w ***załączniku nr 4*** do niniejszej Polityki bezpieczeństwa i stanowi on podstawę do nadania uprawnień do dostępu do systemu informatycznego (***załączniku nr 5)***.
8. Szczegółowa instrukcja nadawania uprawnień zawarta jest w ***„Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Wojewódzkim Szpitalu Psychiatrycznym w Andrychowie”,*** która jest integralną częścią Polityki Bezpieczeństwa.

3.3. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami.

1. Dane osobowe gromadzone są w systemach informatycznych oraz w zbiorach manualnych.
2. Gromadzone dane osobowe są udostępniane pracownikom w zakresie niezbędnym do ich pracy i wynikającym z przepisów prawa poprzez posiadane systemy informatyczne.
3. Zakres pozyskiwanych danych jest adekwatny i ograniczony do minimum niezbędnego do realizacji wskazanego celu.
4. W ramach procesów przetwarzania danych dochodzi do przepływu danych pomiędzy systemami informatycznymi poprzez moduły do przeglądania danych.
5. Możliwość wglądu przez pracowników w dane osobowe pozwala na ich porównywanie i sprostowanie ewentualnych rozbieżności ograniczając jednocześnie ilość wyjaśnień.
6. Struktura zbiorów danych osobowych przetwarzanych w systemach informacyjnych oraz sposób ich przepływu została zawarta w ***załączniku nr 2.***

3.4. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

Zastosowanie środków technicznych i organizacyjnych odnosi się zarówno do danych przetwarzanych w sposób tradycyjny (manualny, papierowy), jak i do przetwarzania danych w systemach informatycznych.

Do elementów zabezpieczenia danych osobowych w Szpitalu składają się w szczególności:

1. Procedura nadawania/odwołania upoważnień do przetwarzania danych.
2. Opis zastosowanych zabezpieczeń technicznych.
3. Opis zastosowanych zabezpieczeń organizacyjnych.
4. Procedura postępowania przy naruszeniu ochrony danych osobowych
5. Zasady udostępniania danych.
6. Procedury powierzania danych.
7. Obowiązki ASI
8. Obowiązki IOD

1. Procedura nadawania/zmiany/odwołania upoważnień do przetwarzania danych, – o której wspomniano wyżej omówiona została w ***„Instrukcji zarządzania systemem informatycznym …”***

2. Opis zastosowanych zabezpieczeń technicznych:

Zabezpieczenie obszaru (budynków, pomieszczeń), w którym przetwarzane są dane osobowe w formie papierowej lub w systemie informatycznym odbywa się poprzez:

- budynek szpitala wyposażony jest w system kontroli dostępu, uniemożliwiający dostęp osobom nieuprawnionym. Uprawnienia użytkowników nadawane są jedynie w zakresie niezbędnym do wykonywania obowiązków służbowych,
- na terenie Szpitala wprowadzono w monitoring wizyjny. Obejmuje on wejścia do budynków, ciągi komunikacyjne, Izbę Przyjęć, Poradnię Zdrowia Psychicznego,
- obszary o podwyższonym poziomie bezpieczeństwa typu: gabinety lekarskie, laboratorium, administracja wyposażone są w postaci bezpiecznych drzwi; instalację przeciwpożarową, kraty w oknach,
- dla zachowania ciągłości działania zapewnione jest awaryjne źródło zasilania typu generator prądotwórczy oraz urządzenia UPS,
- zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity, użyto system Firewall do ochrony dostępu do sieci komputerowej,
- wykorzystywany sprzęt jest regularnie poddawany konserwacji. Naprawa i konserwacja sprzętu wykonywana jest wyłącznie przez osoby uprawnione ,
- pomieszczenia, w których są przetwarzane są dane osobowe, zamykane są na klucz,
- dostęp do kluczy posiadają tylko upoważnieni pracownicy,
- przetwarzanie danych osobowych ma miejsce w wyznaczonych pomieszczeniach,
- dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy. W sytuacji, gdy jest wymagany poza godzinami pracy - możliwy jest tylko na podstawie zezwolenia administratora danych,
- dostęp do pomieszczeń, w których są przetwarzane dane osobowe, mogą mieć tylko upoważnieni pracownicy
- w przypadku pomieszczeń, do których dostęp mają również osoby nieupoważnione, mogą one przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych i tylko w czasie wymaganym na wykonanie niezbędnych czynności,
- szafy, w których przechowywane są dane, zamykane są na klucz.
- klucze do tych szaf posiadają tylko upoważnieni pracownicy,
- szafy z danymi są otwarte tylko na czas potrzebny na dostęp do danych, a następnie są zamykane,
- dane w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny do wykonania czynności służbowych, a następnie muszą być chowane do szaf,
- dostęp do komputerów, na których są przetwarzane dane, mają tylko upoważnieni pracownicy,
- monitory komputerów, na których przetwarzane są dane, są tak ustawione, aby osoby nieupoważnione nie miały wglądu w dane,
- w razie potrzeby wyniesienia komputera przenośnego czy zewnętrznego nośnika danych zawierającego dane osobowe lub inne informacje chronione, komputer taki musi być odpowiednio dodatkowo zabezpieczony, a dane zaszyfrowane. Ponadto należy wystąpić o zgodę do administratora.

- zabrania się udostępniania osobom nieupoważnionym komputerów przenośnych czy zewnętrznych nośników danych,
- w razie potrzeby przeniesienia danych osobowych pomiędzy komputerami należy zrobić to z zachowaniem szczególnej ostrożności,
- nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie), aby nie zostały na nich dane osobowe,
- jeśli nie ma możliwości skasowania danych z nośnika (np. płyta CD-ROM), należy go zniszczyć fizycznie,
- niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną,
- wydruki komputerowe zawierające dane osobowe, a przeznaczone do likwidacji, są niszczone w sposób bezpowrotny tak, aby nie było możliwe odczytanie zamieszczonych na nich informacji (np. w niszczarce dokumentów),
- politykę czystego biurka. W przypadku dłuższej nieobecności przy stanowisku pracy lub po jej zakończeniu pracownik jest zobowiązany do umieszczenia wszelkich dokumentów i nośników zawierających dane osobowe w bezpiecznym miejscu, np. zamykanej szafce, w celu uniemożliwienia dostęp do nich osobom nieuprawnionym. Nie należy również zostawiać dokumentów i nośników w łatwo dostępnych miejscach, np. przy urządzeniach drukujących,
- politykę czystego ekranu: W przypadku opuszczenia stanowiska pracy pracownik jest zobowiązany do wylogowania się z aplikacji lub zablokowania dostępu do pulpitu stacji roboczej, w celu uniemożliwienia dostępu do systemu lub aplikacji osoby nieupoważnionej,
- zasadę rozpoczęcia i zakończenia pracy: Pracownik rozpoczynając pracę powinien zalogować się do systemu/aplikacji, na zakończenie pracy musi się wylogować,

3. Opis zastosowanych zabezpieczeń organizacyjnych:

- opracowano i wdrożono politykę bezpieczeństwa dla pracowników zatrudnionych przy przetwarzaniu danych osobowych,
- opracowano i wdrożono instrukcję zarządzania systemem informatycznym,
- opracowano i wdrożono procedurę zarządzania incydentami cyberbezpieczeństwa
- opracowano i wdrożono procedurę zarządzania ryzykiem w obszarze ochrony danych osobowych
- powołano Administratora Systemów Informatycznych,
- powołano Inspektora Danych Osobowych,
- wprowadzono ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych,
- osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych,
- osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy,
- prowadzona jest bieżąca kontrola stanu bezpieczeństwa systemu informatycznego, w którym przetwarzane są dane osobowe,
- stała kontrola dostępu do pomieszczeń, w których przetwarzane są dane osobowe,
- tworzenie kopii zapasowych baz danych zawierających dane osobowe,
- dokładne testowanie modyfikacji oprogramowania przed wdrożeniem go do użytku operacyjnego zarówno pod kątem poprawności działania jak i podatności na „ataki" z zewnątrz,
- urządzenia wchodzące w skład infrastruktury sieciowej, serwer oraz komputery, na których przetwarzane są dane osobowe podłączone są do awaryjnych zasilaczy UPS, zabezpieczających przed skokami napięcia i zanikiem zasilania.
- w trakcie przetwarzania danych osobowych pracownik jest osobiście odpowiedzialny za bezpieczeństwo powierzonych mu danych,
- przed przystąpieniem do realizacji zadań związanych z przetwarzaniem danych osobowych pracownik winien sprawdzić, czy posiadane przez niego dane były należycie zabezpieczone oraz czy zabezpieczenia te nie były naruszone,
- w trakcie przetwarzania danych osobowych pracownik winien dbać o należyte ich zabezpieczenie przed możliwością wglądu bądź zmiany przez osoby do tego nieupoważnione,
- po zakończeniu przetwarzania danych pracownik winien należycie zabezpieczyć dane osobowe przed możliwością dostępu do nich osób nieupoważnionych.

4. Procedura postępowania przy naruszeniu ochrony danych osobowych

W ***Rozdziale 2*** został zaprezentowany katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych.

Podsumowując przez **naruszenie ochrony danych osobowych** rozumiemy 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.

W przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych ważne jest umiejętne postępowanie z incydentami, reagowanie na zdarzenie oraz sposób komunikowania o zaistniałej sytuacji w organizacji. W tym celu została opracowana ***„Procedura postępowania w sytuacji naruszenia ochrony danych osobowych”***, która stanowi integralną część do Polityki bezpieczeństwa.

„***Procedura***….” Opisuje, co ma zrobić pracownik w przypadku podejrzenia zagrożenia dla poufności danych, np., gdy widzi, że dane w formie papierowej są zabezpieczone niewłaściwie lub podejrzewa, że ktoś może mieć nieuprawniony dostęp do danych w systemie informatycznym.

Zdarzenia mogą być wykrywane przez osoby, które zauważą coś niepokojącego, lub przez urządzenia i środki techniczne, które przesyłają sygnały alarmowe.

Niezależnie od źródła wykrycia zdarzenia naruszenia bezpieczeństwa każda osoba powiadomiona o tym fakcie lub taka, która sama zauważyła coś niezwykłego, jest odpowiedzialna za zainicjowanie dalszego postępowania i za poinformowanie innych. Osoba zgłaszająca zdarzenie powinna sporządzić notatkę, podając jak najwięcej dostępnych informacji. Istotne są nie tylko dokładność i kompletność informacji, niekiedy przede wszystkim czas.

IOD dokumentuje zaistniały przypadek naruszenia oraz sporządza raport. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu IDO podejmuje postępowanie naprawcze. Po przywróceniu prawidłowego stanu bazy danych osobowych przeprowadza analizę w celu określenia przyczyny naruszenia ochrony danych osobowych oraz wprowadza kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości. Jeżeli przyczyną zdarzenia był błąd osoby zatrudnionej przy przetwarzaniu danych osobowych IOD niezwłocznie zarządza przeprowadzenie dodatkowego szkolenia dla osób biorących udział przy przetwarzaniu danych osobowych. Dokumentację z przeprowadzonego szkolenia IOD załącza do raportu. Raport IOD przedkłada niezwłocznie Administratorowi, który wydaje pisemne zalecenia. Całość dokumentacji w zakresie naruszenia systemu ochrony danych osobowych przechowuje IOD.

5. Zasady udostępniania danych.

- Dane osobowe mogą być udostępniane wyłącznie podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa oraz osobom, których dotyczą.
- Informacje zawierające dane osobowe powinny być przekazywane uprawnionym podmiotom lub osobom za potwierdzeniem odbioru listem poleconym za pokwitowaniem odbioru lub innym bezpiecznym sposobem, określonym wymogiem prawnym lub umową.
- Udostępniając dane osobowe innym podmiotom należy odnotowywać informacje o udostępnieniu bezpośrednio w systemie informatycznym, z którego udostępniono dane lub w inny zatwierdzony sposób. Odnotować należy: informacje o odbiorcy danych, dacie i zakresie udostępnionych danych osobowych.
- Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

6. Procedury powierzania danych.

Zgodnie z przepisami o ochronie danych osobowych, administrator danych osobowych może powierzyć przetwarzanie przez siebie dane innej firmie. Podstawą do ich przekazania jest zawarcie stosownej umowy. Firma, której powierzono dane osobowe może je przetwarzać włącznie w zakresie i celu określonym w umowie. W Wojewódzkim Szpitalu Psychiatrycznym w Andrychowie prowadzi się rejestr umów powierzenia.

7. Obowiązki ASI.

- nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w systemach informatycznych,
- prowadzenie i aktualizacja rejestru nadanych uprawnień do przetwarzania danych w systemach informatycznych,
- nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych
- w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,
- podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,
- identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych i tradycyjnych,
- sprawowanie nadzoru nad przechowywanymi kopiami zapasowymi,
- inicjowanie i nadzór nad wdrażaniem nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które mają doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych,
- nadzór nad naprawą oraz likwidacją urządzeń komputerowych,
- kontrola przeglądu i konserwacji systemów informatycznych służących do przetwarzania danych osobowych,
- zabezpieczenie systemów służących do przetwarzania danych osobowych przed działaniem oprogramowania złośliwego,
- podejmowanie innych czynności w zakresie zabezpieczenia przetwarzania danych w systemach informatycznych, o których mowa w ***„Instrukcji zarządzania systemem informatycznym …”***
- informowanie Administratora o konieczności wprowadzenia zmian (z powodu np. zmian procedur tworzenia kopii zapasowych lub zmiany zabezpieczeń systemów informatycznych),
- inne czynności wskazane w niniejszej *Polityce oraz Instrukcji*.

8. Obowiązki IOD.

- monitorowanie przestrzegania przepisów o ochronie danych osobowych oraz wewnętrznych dokumentów, procedur firmy i zaleceń dla przetwarzania danych, a także bieżące informowanie kierownictwa o wnioskach,
- przeprowadzanie audytów zgodności przetwarzania danych osobowych z przepisami oraz opracowywanie sprawozdań i zaleceń dla kierownictwa,
- informowanie pracowników oraz współpracowników o ich obowiązkach wynikających z przepisów o ochronie danych oraz przyjmowanie od nich oświadczenia o zachowaniu poufności,
- informowanie kierownictwa o obowiązkach wynikających z przepisów o ochronie danych, w tym aktywne doradzanie, jakie działania powinny być podejmowane,
- przeprowadzanie analizy ryzyka i zagrożeń oraz przedstawianie wniosków i zaleceń kierownictwu,
- organizowanie szkoleń wstępnych i okresowych z ochrony danych osobowych,
- pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, w tym przygotowywanie odpowiedzi na ich żądanie i udzielanie odpowiedzi,
- wsparcie administratora oraz pracowników w realizacji żądań osób, których dane dotyczą,
- monitorowanie udostępnień danych osobowych, w tym wydawanie opinii w zakresie realizacji wniosku o udostępnienie,
- pełnienie funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych,

- aktywne wsparcie kierownictwa w przypadku naruszenia poufności poprzez przygotowanie odpowiednich zaleceń działań, określenie poziomu ryzyka dla naruszenia praw i wolności, przeprowadzenie audytu, wsparcie przy zgłoszeniu naruszenia oraz udzielaniu wyjaśnień z tym związanych,
- aktywne włączenie się we wszelkie sprawy związane z przetwarzaniem danych osobowych,
- nadzór nad aktualnością dokumentacji i wewnętrznych procedur zarządzania bezpieczeństwem danych osobowych, w tym proponowanie nowych procedur.

Rozdział 4

Postanowienia końcowe

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu, w szczególności przez osobę, która wobec naruszenia ochrony danych osobowych lub uzasadnionego domniemania takiego naruszenia, nie podjęła działań określonych w niniejszym dokumencie, mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych.
2. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie.
3. Wdrożenie „Polityki bezpieczeństwa" odbywa się poprzez zapoznanie osób wchodzących w skład organów organizacji, pracowników, współpracowników, wolontariuszy, praktykantów i stażystów organizacji z treścią „Polityki bezpieczeństwa".
4. Osoby, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych, potwierdzają ten fakt poprzez podpisanie oświadczenia.
5. Ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych, zobowiązany jest prowadzić IOD.
6. Wszystkie regulacje dotyczące systemów informatycznych określone w „Polityce bezpieczeństwa" dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
7. „Polityka bezpieczeństwa" wchodzi w życie z dniem podpisania Zarządzenia Dyrektora Wojewódzkiego Szpitala Psychiatrycznego w Andrychowie.

Załącznik nr 1

Wykaz pomieszczeń tworzących obszar przetwarzania danych osobowych w systemie informatycznym w Wojewódzkim Szpitalu Psychiatrycznym w Andrychowie

Komórka organizacyjna przetwarzająca dane osobowe w systemie informatycznym	Pomieszczenie, w którym przetwarzane są dane osobowe
Dyrektor WSP	segment AII, II piętro, 3.43
Sekretariat	segment AII, II piętro, 3.42
Dyr. ds. Lecznictwa, Prawnik	segment AII, II piętro, 3.47
Główny Księgowy	segment AII, II piętro, 3.40
Dział Finansowo-Księgowy	segment AII, II piętro, 3.38
Kasa	segment AII, II piętro, 3.36
Dział Organizacyjno Personalny	segment AII, II piętro, 3.44, 3.45
Dział Inwestycji i Funduszy Zewnętrznych, IOD, OC	segment AII, II piętro, 3.39
Dział Techniczno-Zaopatrzeniowy	segment AII, parter, 1.41; 1.40
Dział Statystyki i Zarządzania Informacją	segment AI, poddasze, 1.6, 1.7, 1.8
Pracownia Diagnostyki Laboratoryjnej	segment AII, I piętro, 2.56
Apteka Szpitalna	segment AII, I piętro, 2.41, 2.36
Przełożona Pielęgniarek	segment C, parter,1.107
Pielęgniarka epidemiologiczna, Pracownik socjalny, Pracownik BHP	segment C, parter,pok.1.108
Izba Przyjęć Szpitala	segment B, parter, 1.77
Oddział Leczenia Alkoholowych Zespołów Abstynencyjnych	segment C,D, parter, 1.146, 1.143, 1.142
Oddział Psychogeriatryczny	segment C, parter 1.111, 1.109, 1.114
Oddział Terapii Uzależnienia od Alkoholu	segment F, parter, 1.30, 1.36, 1.20 segment F, I piętro, 2.37, 1.37
Oddział Dzienny Terapii Uzależnień Bliżej Niescharakteryzowanych, Poradnia Terapii Uzależnienia Od Alkoholu I Współuzależnienia	segment AII, parter, 1.46, 1.59, 1.62, 1.47
Oddziały Psychiatryczne CZP	segment AI, I piętro, 2.24, 2.23, 2.22, , 2,21 segment C, I piętro, 2.68, 2.69, 2.71, 2,72, 2,77
Oddział Dzienny Psychiatryczny CZP	segment AI, II piętro, 3.24, 3.22
Poradnia Zdrowia Psychicznego	segment B, parter, 1.83, 1.79, 1.86, 1.87, 1.88
Zespół Leczenia Środowiskowego CZP	segment AI, parter, 1.25, 1.27
Informatyk, Serwerownia	Segment AI, AII, D,F

Załącznik nr 2

Wykaz zbiorów danych osobowych w Wojewódzkim Szpitalu Psychiatrycznym w Andrychowie wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych

L.p.	Zbiór danych osobowych	Nazwa systemu/programu służącego do przetwarzania danych osobowych	Zawartość poszczególnych pól informacyjnych i powiązania między nimi	Sposób przepływu danych	Dział /Oddział
1	FK/Koszty	ADM	**Zakres:** Imię i nazwisko, adres zamieszkania, data i miejsce urodzenia, nr konta bankowego	Brak przepływu danych	FK
2	Kadry – Płace	ADM/	**Zakres:** Imię i nazwisko, dane adresowe, dane o wykształceniu, przebiegu pracy, absencji, zakres obowiązków, stawki wynagrodzenia, kary, nagrody	Ewidencja papierowa > program Kadry Płace > Bank	OP
3	Dane osobowe dotyczące obecnych i byłych pracowników	Papierowo – Akta osobowe		Brak przepływu danych	OP
4	Płatnik	WSP	**Zakres:** Imię i nazwisko, dane adresowe, dane o kadrowe (lata pracy, stawki wynagrodzeń) dane o czasie pracy, nagrodach, potrąceniach, zajęciach komorniczych, nr kont dla przelewów bankowych	Ewidencja papierowa > program Płatnik > ZUS	OP
5	Pracownicy	BHP	**Zakres:** Imię i nazwisko, data zatrudnienia, data i miejsce urodzenia, miejsce zamieszkania	Brak przepływu danych	BHP
6	Pacjenci	SZP	**Zakres:** nr,księgi głównej, imię i nazwisko, PESEL, płeć, data urodzenia, miejsce zamieszkania, stan cywilny, nr.dowodu osobistego, nr.dowodu potwierdzającego ubezpieczenie, data i godzina przyjęcia, nazwa i kod instytucji kierującej, nr.umowy z NFZ., regon tej instytucji, skierowania, imię i nazwisko lekarza kierującego i przyjmującego, nazwa i kod rozpoznania, choroby współistniejące, data wypisu, rozpoznanie, dokąd wypisany, wykształcenie, źródło utrzymania, inform.o pobycie i otrzymania kserokopii dokumentacji medycznej, tryb wypisu, lekarz wypisujący, ilość dni pobytu	Ewidencja papierowa > program SZP > NFZ	SIZI, IP, PZP, ODTUB
7	Pacjenci	RUCH	**Zakres:** nr.księgi głównej, imię i nazwisko, PESEL, płeć, data urodzenia, miejsce zamieszkania, stan cywilny, nr.dowodu osobistego, nr.dowodu potwierdzającego ubezpieczenie, data i godzina przyjęcia, nazwa i kod instytucji kierującej, nr.umowy z NFZ., regon tej instytucji, skierowania, imię i nazwisko lekarza kierującego i przyjmującego, nazwa i kod rozpoznania, choroby współistniejące, data wypisu, rozpoznanie, dokąd wypisany,	Brak przepływu danych	SIZI

			wykształcenie, źródło utrzymania, inform.o pobycie i otrzymania kserokopii dokumentacji medycznej		
8	Ewidencja wyposażenia	SZP WYPOSAŻENIE	**Zakres:** Imię i nazwisko, oddział	Brak przepływu danych	FK, DTZ
9	Dokumentacja medycznej	papierowo	**Zakres:** Imię i nazwisko, PESEL, adres zamieszkania,nr księgi głównej, nr księgi oddziału,data przyjęcia, rozpoznanie wstępne i przy wypisaniu z oddziału, nr statystyczny choroby, data wypisania	Sąd, prokuratura, inne organy	Oddziały / Poradnie
10	Organizacja pracy	papierowo	**Zakres:** Imię i nazwisko, oddział	Brak przepływu danych	Oddziały / Poradnie / Działy
11	Ewidencja wniosków o wydanie dokumentacji medycznej	papierowo	**Zakres:** Imię i nazwisko wnioskodawcy, PESEL, adres zamieszkania, imię i nazwisko pacjenta, PESEL pacjenta	Brak przepływu danych	Oddziały / Poradnie /SIZI
12	Pełnomocnictwa, upoważnienia, wzory podpisów	papierowo	**Zakres:** Imię i nazwisko, imiona rodziców, data i miejsce urodzenia, seria i numer dowodu osobistego, PESEL, adres zamieszkania, identyfikator, miejsce pracy,	Brak przepływu danych	OP
13	Ewidencja zabezpieczeń	elektronicznie Windows	**Zakres:** Imię i nazwisko, oddział	Brak przepływu danych	OP
14	Ewidencja upoważnień do przetwarzania danych	elektronicznie Windows	**Zakres:** Imię i nazwisko,	Brak przepływu danych	IOD
15	Umowy zlecenia /cywilno - prawne	papierowo	**Zakres:** Imię i nazwisko, PESEL, adres zamieszkania, **NIP i REGON, adresy siedzib (firmy)**	Brak przepływu danych	OP/DTZ
16	Archiwum Szpitala	papierowo	**Zakres: (Pacjent)** imię i nazwisko, PESEL ,płeć, data urodzenia, miejsce zamieszkania, stan cywilny, nr.dowodu osobistego, nr.dowodu potwierdzającego ubezpieczenie, data i godzina przyjęcia, nazwa i kod instytucji kierującej, nr.umowy z NIZ., regon tej instytucji, skierowania, imię i nazwisko lekarza kierującego i przyjmującego, nazwa i kod rozpoznania, choroby współistniejące, data wypisu, rozpoznanie, dokąd wypisany,	Brak przepływu danych	DTZ
17		papierowo	**Zakres (Pracownik):** Imię i nazwisko, dane adresowe, dane o wykształceniu, przebiegu pracy, absencji, zakres obowiązków, stawki wynagrodzenia, kary, nagrody		
18	Ewidencja zamówień, usterek, wydawanych rzeczy z magazynów	papierowo/ elektronicznie Windows	**Zakres:** Imię i nazwisko, oddział	Brak przepływu danych	DTZ

19	Dane osobowe z zakresu przygotowań obronnych Szpitala	papierowo	**Zakres:** Imię i nazwisko, adres zamieszkania	Brak przepływu danych	OC
20	Dokumentacja Stałego Dyżuru	elektronicznie Windows / papierowo	**Zakres:** Imię i nazwisko, numer telefon, pełniona funkcja, adres zamieszkania	Ewidencja papierowa > UMWM	OC
21	Plan obrony cywilnej	elektronicznie Windows / papierowo	**Zakres:** Imię i nazwisko, numer telefon, pełniona funkcja, adres zamieszkania	Ewidencja papierowa > UM	OC

Załącznik nr 3

Ewidencja osób upoważnionych do przetwarzania danych osobowych

Lp.	Imię i nazwisko	Numer upoważnienia	Data nadania uprawnień	Data ustania uprawnień	Zakres upoważnienia(1)	Identyfikator */jeśli dotyczy/*	Uwagi

(1)Skróty stosowane do zakresu upoważnienia:
Z – pełne prawa do zarządzania bazą danych
W – pełne prawa do edycji danych (w tym drukowania, archiwizowania, usuwania)
N – prawo do zakładania nowych kont
M – prawo do dodawania i modyfikacji danych
P – prawo do przeglądania danych na monitorze
D – prawo do drukowania danych
A – prawo do wykonywania kopii archiwalnych
FP – przetwarzanie danych w formie papierowej

Dane aktualne na dzień: ……..……

……..
/Pieczątka i podpis Dyrektora Szpitala)

Załącznik nr 4

Upoważnienie nr
do przetwarzania danych osobowych

1. *Na podstawie art. 29 i art.5 ust.1 lit.f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych)* upoważniam Panią/Pana **……..** zatrudnioną/nego na podstawie umowy o pracę/umowy cywilnoprawnej na stanowisku **……..** w Wojewódzkim Szpitalu Psychiatrycznym w Andrychowie.
2. Upoważnienie obejmuje przetwarzanie danych osobowych na wyznaczonym stanowisku pracy, zgodnie z powierzonymi obowiązkami pracowniczymi oraz poleceniami służbowymi.
3. Jednocześnie zobowiązuję Panią/Pana do zachowania w tajemnicy (również po odwołaniu upoważnienia, a także ustaniu stosunku zatrudnienia) danych osobowych uzyskanych w trakcie dokonywania operacji związanych z ich przetwarzaniem oraz sposobów ich zabezpieczania.
4. Niniejsze upoważnienie ważne jest od dnia …….r. i wygasa z dniem ustania stosunku pracy, a ponadto może być w każdym czasie zmienione lub odwołane.

……. ……..…….
(Podpis upoważnionego) (Pieczątka i podpis Dyrektora Szpitala)

Oświadczenie

Oświadczam, że zapoznałam/em się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi w Wojewódzkim Szpitalu Psychiatrycznym w Andrychowie. Zobowiązuję się do zachowania w tajemnicy wszelkich informacji o danych osobowych uzyskanych w trakcie dokonywania operacji związanych z przetwarzaniem danych osobowych oraz informacji o ich zabezpieczeniu. Powyższej tajemnicy zobowiązuję się dochować również po zakończeniu zatrudnienia. Jestem świadoma/y, że naruszenie poufności przetwarzanych danych osobowych może nieść dla mnie konsekwencje dyscyplinarne.

…….
(Podpis upoważnionego)

- niniejsze upoważnienie zostało sporządzone w dwóch jednobrzmiących egzemplarzach, które otrzymują:
1. Osoba upoważniona.
2. Dział Organizacyjno Personalny – do akt osobowych upoważnionego.

Załącznik nr 5

Uprawnienia dostępu do systemu informatycznego

Dane użytkownika:

Imię i nazwisko	
Stanowisko służbowe	
Telefon, e-mail	
Nr upoważnienia do przetwarzania danych osobowych	

Uprawnienia dotyczą systemu informatycznego :

Zakres	**Nazwa systemu informatycznego, w którym dane są przetwarzane**	**Zakres uprawnień związanych z dostępem do systemu** *(np. podgląd / odczyt/edycja….)*

Uprawnienia będą przyznane:*)

[ ] na okres od ..... r. do ..... r. *)

[ ] na czas trwania upoważnienia do przetwarzania danych)

Adnotacje Administratora Systemu Informatycznego

Nadany identyfikator:

Uwagi:

.....

Data i podpis Administratora Systemu Informatycznego

- niniejsze upoważnienie zostało sporządzone w dwóch jednobrzmiących egzemplarzach, które otrzymują:
1. Osoba upoważniona.
2. IOD

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Wojewódzkim Szpitalu Psychiatrycznym w Andrychowie

Rozdział 1.
Wprowadzenie

Podstawę prawną dla opracowania i wdrożenia niniejszej instrukcji stanowi:

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016r. w sprawie ochrony osób fizycznych oraz rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29.04.2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. 2004.100.1024).

Instrukcja użytkowania systemem informatycznym, służącym do przetwarzania danych osobowych, zwana dalej „instrukcją", jest wewnętrznym dokumentem administratora danych osobowych Wojewódzkiego Szpitala Psychiatrycznego w Andrychowie, skierowanym do osób zatrudnionych w WSP.

Wszelkie przypadki naruszenia zasad i reguł zawartych w niniejszej instrukcji należy zgłaszać administratorowi danych lub bezpośredniemu przełożonemu.

Rozdział 2.
Procedury nadawania uprawnień do przetwarzania danych osobowych i rejestrowanie tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

1. Do obsługi systemu informatycznego służącego do przetwarzania danych osobowych, dopuszczona jest wyłącznie osoba posiadająca upoważnienia do przetwarzanie danych osobowych wydane przez administratora danych.
2. Rejestracji użytkownika systemu informatycznego dokonuje się na podstawie upoważnienia, o którym mowa w pkt 1.
3. Rejestracji użytkownika w systemie dokonuje administrator systemu informatycznego zwany dalej Informatyk.
4. Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora użytkownika i właściwego hasła. Identyfikator i hasło jednoznacznie identyfikują, weryfikują i autoryzują tożsamość użytkownika.
5. Dla każdego użytkownika systemu informatycznego, który przetwarza dane osobowe, administrator systemu informatycznego ustala niepowtarzalny identyfikator i hasło początkowe.
6. Identyfikator użytkownika jest niezmienny, a po wyrejestrowaniu użytkownika z systemu informatycznego, nie jest usuwany.
7. Użytkownikom nadawane są uprawnienia do pracy tylko w wymaganych dla realizacji powierzonych zadań modułach i funkcjach programów.
8. Za realizację procedury rejestrowania i wyrejestrowania użytkowników w systemie informatycznym odpowiedzialny jest Informatyk.
9. Administrator danych prowadzi ewidencję osób upoważnionych przez niego do przetwarzania danych osobowych w systemie informatycznym, zawierającą: imię i nazwisko, datę nadania uprawnień, datę ustania uprawnień, zakres upoważnienia, identyfikator.
10. Unieważnienie upoważnienia następuje z dniem ustania stosunku pracy, stażu, praktyki lub na polecenie przełożonego. Fakt ten zostaje odnotowywany w ewidencji upoważnień i przekazany do informatyka o konieczności odcięcia wszelkich dostępów i odzyskania sprzętu informatycznego.

Służbowa poczta elektroniczna

1. Pierwsze hasło jest nadawane Pracownikowi przez Administratora Systemów Informatycznych.
2. Pracownik powinien zabezpieczyć dostęp do służbowej poczty elektronicznej (służbowego adresu e-mail) poprzez nadanie jej indywidualnego silnego hasła ochronnego.
3. Pracownik powinien chronić hasło przed dostępem osób trzecich. W każdym przypadku, gdy hasło zostało ujawnione innej osobie, Pracownik jest zobowiązany do jego zmiany.
4. Pracownik powinien wykorzystywać służbową pocztę elektroniczną (służbowy adres e- mail) jedynie do czynności związanych z wykonywaną pracą.
5. Zabronione jest wykorzystywanie prywatnej poczty elektronicznej (prywatnego adresu e-mail) do celów służbowych.
6. Pracownik jest zobowiązany do korzystania z przyznanego mu adresu mailowego do wszelkiej korespondencji służbowej z innymi pracownikami placówki.
7. Pracownik posiadający adres mailowy zobowiązany jest do:

- sprawdzania systematycznie, na bieżąco skrzynki pocztowej każdego dnia, w którym jest obecny w pracy i wykonuje obowiązki służbowe;
- odpowiadania na e-mail'e;
- uważać na wszelkie linki, załączniki w wiadomościach mailowych, zwłaszcza te sugerujące podjęcie jakiegoś działania, np. konieczność zmiany hasła, albo podejrzaną aktywność na koncie lub takich których nie spodziewaliśmy się dostać. W przypadku otrzymania podejrzanego e-maila, poprośmy informatyka o sprawdzenie;
- należy sprawdzać rzeczywisty adres e-mail nadawcy wiadomości – czy domena w adresie pochodzi faktycznie z organizacji wysyłającego. Nie należy kierować się tylko nazwą użytkownika;
- przesyłane załączniki powinny być szyfrowane, a ustawiane hasła wysyłane innym kanałem komunikacji;
- nie należy zamieszczać niezanonimizowanych danych osobowych ani innych wrażliwych informacji w treści wiadomości;
- logując się do poczty ustawiajmy długie i złożone hasła.

8. Pracownik zobowiązuje się, że nie będzie działał w sposób naruszający prawa innych użytkowników systemu pocztowego oraz nie będzie przenosił prawa do korzystania ze swojej skrzynki pocztowej na osoby trzecie.
9. Pracownik ma prawo korzystać ze służbowego konta pocztowego w pełnym zakresie jego funkcjonalności pod warunkiem, że będzie to zgodne z obowiązującym prawem, normami społecznymi i obyczajowymi.
10. Pracownik powinien stosować odpowiednie środki ostrożności zapobiegające wprowadzeniu wirusów do systemu poczty elektronicznej.

Rozdział 3.
Stosowane metody i środki uwierzytelniania oraz procedury związane z zarządzaniem nimi i ich użytkowaniem

1. Każdorazowe uwierzytelnienie użytkownika w systemie następuje po podaniu identyfikatora i hasła.
2. Używanie hasła jest obowiązkowe dla każdego użytkownika posiadającego identyfikator w systemie.
3. Użytkownik jest w pełnym zakresie odpowiedzialny za swoje hasło, w tym za jego okresowe zmienianie i utrzymywanie w tajemnicy, również po upływie jego ważności.
4. Użytkownik jest w pełnym zakresie odpowiedzialny za dostosowanie hasła do niżej obowiązujących reguł, jeśli przestrzeganie tych reguł nie wymusza w sposób automatyczny system informatyczny lub oprogramowanie.
5. Hasło użytkownika nie może być takie samo jak identyfikator użytkownika.
6. Hasło użytkownika musi składać się, z co najmniej 8 znaków, wskazane jest, by zawierało małe i duże litery oraz cyfry lub znaki specjalne.
7. Hasło użytkownika powinno być zmieniane nie rzadziej, niż co 30 dni. W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest do

natychmiastowej zmiany hasła, lub w razie problemów powiadomić o tym fakcie administratora systemu informatycznego.
8. Hasło wpisywane z klawiatury nie może pojawiać się na ekranie monitora w formie jawnej.
9. Hasło nie może zawierać żadnych informacji, które można kojarzyć z użytkownikiem systemu informatycznego.
10. Zabrania się zapisywania hasła lub takiego z nim postępowania, które umożliwia lub ułatwia dostęp do hasła osobom trzecim.
11. Administrator systemu informatycznego nadaje hasło początkowe.
12. Użytkownik otrzymuje hasło początkowe przy przystąpieniu do pracy w systemie informatycznym i jest zobowiązany zmienić je natychmiast po rozpoczęciu pracy na tylko sobie znany ciąg znaków. Administrator systemu informatycznego zobowiązany jest dopilnować lub wymusić w systemie zmianę hasła początkowego.
13. Administrator systemu informatycznego musi mieć możliwość zmiany hasła użytkownika bez znajomości aktualnego lub nieważnego hasła użytkownika.
14. Obowiązuje bezwzględny zakaz notowania w jakiejkolwiek formie obecnych lub wygasłych haseł dostępu.

Rozdział 4.
Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

1. Przed przystąpieniem do pracy w systemie informatycznym użytkownik zobowiązany jest sprawdzić urządzenie komputerowe i stanowisko pracy oraz zwrócić uwagę, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych. W przypadku naruszenia ochrony danych osobowych użytkownik niezwłocznie powiadamia administratora danych.
2. Użytkownik rozpoczyna pracę w systemie informatycznym od następujących czynności:
- włączenia komputera,
- uwierzytelnienia się („zalogowania" w systemie) za pomocą identyfikatora i hasła.
3. Niedopuszczalne jest uwierzytelnianie się na hasło i identyfikator innego użytkownika lub praca w systemie informatycznym na koncie innego użytkownika.
4. W przypadku konieczności czasowego opuszczenia stanowiska pracy przyłączonego do sieci informatycznej lub służącego przetwarzaniu danych wiążącego się ze stratą pola widzenia swojego stanowiska, użytkownik powinien: wylogować się z programu lub sieci informatycznej, lub zablokować stację roboczą odpowiednią kombinacją klawiszy, przy czym odblokowanie może nastąpić dopiero po podaniu hasła, lub dopilnować konfiguracji wygaszacza ekranu w ten sposób, aby powrót do pracy był możliwy dopiero po podaniu hasła.
5. Zakończenie pracy użytkownika w systemie następuje po poprawnym „wylogowaniu się" z systemu.
6. Niedopuszczalne jest zakończenie pracy w systemie bez wykonania pełnej i poprawnej operacji wylogowania i poprawnego zamknięcia systemu. Po zakończeniu pracy użytkownik zabezpiecza swoje stanowisko pracy, w szczególności dyskietki, pendrive, płyty CD, DVD, taśmy magnetyczne, karty pamięci, dokumenty i wydruki zawierające dane osobowe, przed dostępem osób nieuprawnionych.
7. Przebywanie osób nieuprawnionych w pomieszczeniach znajdujących się w obszarze, w którym są przetwarzane dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania.
8. Użytkownik jest zobowiązany do zadbania, aby niemożliwe było odczytanie informacji z ekranu monitora przez osoby nieuprawnione.
9. Pomieszczenia, w których przetwarzane są dane osobowe, należy zamykać, na czas nieobecności osoby upoważnionej, w sposób uniemożliwiający dostęp do nich osób nieuprawnionych.
10. Użytkownik zobowiązany jest do bezzwłocznego powiadomienia administratora danych w przypadku braku możliwości zalogowania się na swoje konto oraz w przypadku podejrzenia fizycznej ingerencji w przetwarzane dane osobowe lub użytkowane narzędzia programowe i sprzętowe.

Rozdział 5.
Procedury tworzenia kopii zapasowych, zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Celem procedury jest określenie zasad tworzenia, przechowywania i odtwarzania kopii bezpieczeństwa.
2. Procedura przeznaczona jest dla osób przez niego upoważnionych i ma zastosowanie do wszystkich systemów informatycznych eksploatowanych w jednostce, przetwarzających informacje prawnie chronione, w szczególności:

- system obsługi „części białej", w którym są gromadzone dane medyczne,
- system kadrowo-płacowy i finansowo-księgowy,
- inne, krytyczne dla jednostki ochrony zdrowia systemy z punktu widzenia ciągłości działania.

3. Zbiory danych w systemie informatycznym są zabezpieczone przed utratą lub uszkodzeniem za pomocą:

- urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej,
- sporządzania kopii zapasowych zbiorów danych.

4. Na potrzeby zachowania ciągłości działania systemów informatycznych i utrzymania integralności danych wykonuje się kopie zapasowe zbiorów danych. Kopie zapasowe są tworzone, przechowywane oraz wykorzystywane z uwzględnieniem następujących zasad:

- wykonywane są co 24h w godzinach nocnych,
- wykonywane są przez kopiowanie całości danych,
- po wykonaniu kopii zapasowej i awaryjnej administrator systemu informatycznego ma obowiązek sprawdzić poprawność i kompletność skopiowanych danych,

5. Za sporządzanie i bezpieczeństwo kopii zapasowych i awaryjnych odpowiedzialna jest firma, z którą Szpital ma podpisaną umowę serwisową.

Rozdział 6.
Sposób, miejsce i okres przechowywania wydruków, elektronicznych nośników informacji oraz kopii zapasowych zawierających dane osobowe

1. Bieżące wydruki należy przechowywać w szafach zamykanych na klucz w pomieszczeniach, a uniemożliwiających dostęp do nich przez osoby nieupoważnione.
2. Za bezpieczeństwo danych zapisanych w komputerach przenośnych oraz w innych urządzeniach przenośnych w całości odpowiada użytkownik komputera lub urządzenia przenośnego.
3. Osoba zatrudniona przy przetwarzaniu danych osobowych, sporządzająca wydruk zawierający dane osobowe, ma obowiązek na bieżąco sprawdzać przydatność wydruku w wykonywanej pracy, a w przypadku jego nieprzydatności – niezwłocznie wydruk zniszczyć w niszczarce dokumentów.
4. Kopie zapasowe wykonywane na elektronicznych nośnikach przechowywane są w innych pomieszczenia niż te, w których przechowywane są zbiory danych osobowych wykorzystywane na bieżąco. Kopie zapasowe przechowuje się w sposób uniemożliwiający nieuprawnione przejęcie, modyfikacje, uszkodzenie lub zniszczenie.
5. Okres przechowywania ustala administrator danych, zależnie od rodzaju danych, w oparciu o ocenę ich przydatności i obowiązujące przepisy prawa.
6. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe po ustaniu ich użyteczności są pozbawiane danych lub zniszczone w sposób uniemożliwiający odczyt danych.
7. Za zniszczenie zbędnych wydruków i innych zbędnych dokumentów zawierających dane osobowe odpowiedzialny jest kierownik komórki organizacyjnej.

Rozdział 7.
Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1. W związku z istnieniem zagrożenia dla zbiorów danych osobowych, ze strony wirusów komputerowych, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, konieczna jest ochrona sieci komputerowej i stanowisk komputerowych.
2. Przeciwdziałanie zagrożeniom ze strony wirusów komputerowych i szkodliwemu oprogramowaniu realizowane jest następująco:

- komputer z dostępem do internetu musi być zabezpieczony za pomocą oprogramowania antywirusowego.
- zainstalowany program antywirusowy powinien być tak skonfigurowany, by co najmniej raz w tygodniu dokonywał aktualizacji bazy wirusów oraz co najmniej raz w tygodniu dokonywane było automatycznie sprawdzenie komputera pod kątem obecności wirusów komputerowych.
- elektroniczne nośniki informacji takie jak dyskietki, dyski przenośne, należy każdorazowo sprawdzać programem antywirusowym przed użyciem, po zainstalowaniu ich w systemie. Czynność powyższą realizuje użytkownik systemu. W przypadku problemów ze sprawdzeniem zewnętrznego nośnika danych użytkownik jest zobowiązany zwrócić się z tym do Informatyka.
- komputery i systemy pracujące muszą mieć zainstalowany program antywirusowy a w przypadku komputerów z dostępem do Internetu, również posiadać oprogramowanie i mechanizmy zabezpieczające przed nieautoryzowanym dostępem z sieci (firewall)
- w przypadku, gdy użytkownik stanowiska komputerowego zauważy komunikat oprogramowania zabezpieczającego system wskazujący na zaistnienie zagrożenia lub rozpozna tego typu zagrożenie, zobowiązany jest zaprzestać jakichkolwiek czynności w systemie i niezwłocznie skontaktować się z Informatykiem.
- przy korzystaniu z poczty elektronicznej należy zwrócić szczególną uwagę na otrzymywane załączniki dołączane do treści wiadomości. Zabrania się otwierania załączników i wiadomości poczty elektronicznej od „niezaufanych" nadawców.
- zabrania się użytkownikom komputerów, wyłączania, blokowania odinstalowywania programów zabezpieczających komputer (skaner antywirusowy, firewall) przed oprogramowaniem złośliwym oraz nieautoryzowanym dostępem.

Rozdział 8.
Udostępnianie danych osobowych i sposób odnotowania informacji o udostępnionych danych

1. Dane osobowe mogą być udostępniane wyłącznie podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa oraz osobom, których dotyczą.
2. Informacje zawierające dane osobowe powinny być przekazywane uprawnionym podmiotom lub osobom za potwierdzeniem odbioru listem poleconym za pokwitowaniem odbioru lub innym bezpiecznym sposobem, określonym wymogiem prawnym lub umową.
3. Udostępniając dane osobowe innym podmiotom należy odnotowywać informacje o udostępnieniu bezpośrednio w systemie informatycznym, z którego udostępniono dane lub w inny zatwierdzony sposób. Odnotować należy: informacje o odbiorcy danych, dacie i zakresie udostępnionych danych osobowych.
4. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

Rozdział 9.
Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji do przetwarzania danych

1. Przeglądy i konserwację systemu informatycznego należy wykonywać w sposób uniemożliwiający naruszenie ochrony danych osobowych.
2. Przeglądy i konserwacje zbiorów danych dokonywane są poprzez:

- badanie spójności bazy danych,
- analizę zgłaszanych uwag użytkowników.

3. Przed przystąpieniem do przeglądu i konserwacji systemu informatycznego należy sporządzić kopie zapasowe zgodnie z rozdziałem 5 instrukcji.
4. Przeglądy i konserwacje systemu informatycznego mogą być wykonywane wyłącznie przez osoby upoważnione przez administratora danych.
5. Bezwzględnie zabronione jest samodzielne dokonywanie przez użytkowników napraw sprzętu informatycznego, wymiana jego podzespołów oraz wykonywanie innych czynności nie związanych bezpośrednio z jego eksploatacją lub nie dopuszczonych do wykonywania przez producenta sprzętu w instrukcji obsługi.
6. W przypadku zlecenia wykonywania czynności, o których mowa wyżej, podmiotowi zewnętrznemu, wszelkie prace powinny odbywać się pod nadzorem użytkownika lub administratora systemu informatycznego.
7. W przypadku konieczności naprawy poza miejscem użytkowania, sprzęt komputerowy, przed oddaniem do serwisu, powinien być odpowiednio przygotowany. Dane należy zarchiwizować na nośniki informacji, a dyski twarde, bezwzględnie wymontować na czas naprawy.

Rozdział 10.
Regulamin użytkowania komputerów przenośnych oraz zewnętrznych nośników danych

1. Pracownicy upoważnieni do przetwarzania danych osobowych i pracujący na komputerach przenośnych oraz na zewnętrznych nośników danych muszą zapoznać się z Regulaminem użytkowania oraz pisemnego zobowiązania się do jego przestrzegania.
2. Dane osobowe lub dane poufne muszą zostać zaszyfrowane na dysku i zabezpieczone, co najmniej 8-znakowym hasłem (duże, małe litery i cyfry).
3. Komputery przenośne/zewnętrzne nośniki danych są wykorzystywane do prac służbowych. W przypadku konieczności korzystania w innym celu wszystkie dane osobowe muszą być zabezpieczone hasłem.
4. Pracownik zobowiązuje się podejmować wszelkie niezbędne czynności w celu ochrony sprzętu przed kradzieżą.
5. W przypadku kradzieży/zgubienia lub naruszenia ochrony danych osobowych osoba upoważniona zobowiązana jest zgłosić zdarzenie/problem administratorowi.
6. Osoba upoważniona zobowiązana jest do zabezpieczenia komputera przenośnego/zewnętrznego nośnika danych w czasie transportu.
7. Gdy komputer przenośny/zewnętrzny nośnik danych jest pozostawiony w miejscu dostępnym dla osób nieupoważnionych, konieczne jest zabezpieczenie hasłem. Dotyczy to przede wszystkim zabezpieczenia na stanowisku pracy, podczas przedstawiania prezentacji, szkolenia itp
8. Użytkownik komputera przenośnego/zewnętrznego nośnika danych jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych na serwerze. Nośniki z takimi kopiami powinny być przechowywane w miejscu zabezpieczonym przed dostępem osób nieupoważnionych.
9. Pracownik zobowiązuje się nie udostępniać powierzonego sprzętu osobom trzecim.
10. Pracownik zobowiązuje się korzystać z powierzonego komputera przenośnego jedynie w zakładzie pracy lub w domu pracownika, w innych zaś miejscach - tylko po uzyskaniu pisemnej zgody pracodawcy.

Rozdział 11.
Ustalenia końcowe

Osobom korzystającym z systemu informatycznego, w którym przetwarzane są dane osobowe zabrania się:

- ujawniania hasła współpracownikom i osobą z zewnątrz,
- udostępniania stanowisk pracy wraz z danymi osobowymi osobom nieuprawnionym,
- udostępniania osobom nieuprawnionym programów komputerowych zainstalowanych w systemie,

- używania oprogramowania w innym zakresie niż pozwala na to umowa licencyjna,
- przenoszenia programów komputerowych, dysków twardych z jednego stanowiska na inne,
- kopiowania danych na nośniki informacji, kopiowania na inne systemy celem wynoszenia ich poza Szpital,
- samowolnego instalowania i używania jakichkolwiek programów komputerowych,
- używania nośników danych niesprawdzonych, niewiadomego pochodzenia lub niezwiązanych z wykonywaną pracą; w przypadku konieczności użycia niesprawdzonych przenośnych nośników danych, należy zgłosić te nośniki, w celu sprawdzenia przeskanowania programem antywirusowym przez administratora systemu informatycznego,
- wykorzystywania sieci komputerowej w celach innych, niż praca,
- tworzenia kopii zapasowych niechronionych hasłem i/lub bez odpowiednich zabezpieczeń miejsca ich przechowywania,

Ponadto zabrania się:

- wyrzucania zbędnych dokumentów zawierających dane osobowe bez uprzedniego ich trwałego zniszczenia,
- pozostawiania dokumentów, kopii dokumentów zawierających dane osobowe w drukarkach, kserokopiarkach itd.
- pozostawiania kluczy w drzwiach, szafach, biurkach, zostawiania otwartych pomieszczeń, w których przetwarza się dane osobowe,
- pozostawiania bez nadzoru osób trzecich przebywających w pomieszczeniach, w których przetwarzane są dane osobowe,
- pozostawiania dokumentów na biurku po zakończeniu pracy, pozostawiania otwartych dokumentów na ekranie monitora,
- ignorowania nieznanych osób z zewnątrz poruszających się w obszarze przetwarzania danych osobowych,
- przekazywania informacji będącymi danymi osobowymi osobom nieupoważnionym.

Konieczne jest:

- posługiwanie się własnym hasłem w celu uzyskania dostępu do systemu informatycznego,
- tworzenie haseł trudnych do odgadnięcia dla innych,
- nie przerywanie procesu skanowania przez program antywirusowy na komputerze,
- wykonywanie kopii zapasowych danych przetwarzanych na stanowisku komputerowym,
- zabezpieczenie sprzętu komputerowego w tym komputerów przenośnych przed kradzieżą.

Każda osoba upoważniona do przetwarzania danych osobowych jest zobowiązana zapoznać się przed dopuszczeniem do przetwarzania danych osobowych z niniejszą instrukcją oraz złożyć stosowne oświadczenie potwierdzające znajomość jej treści.

CZĘŚĆ C.

Procedura postępowania w sytuacji naruszenia ochrony danych osobowych / Procedura reagowania na incydenty

Postępowania ogólne.

1. Procedura niniejsza określa tryb i zasady postępowania osób zatrudnionych przy przetwarzaniu danych osobowych, w przypadku:

- podejrzenia lub stwierdzenia naruszenia ochrony danych osobowych
- stwierdzono naruszenie zabezpieczenia systemu informatycznego,
- stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń danych

2. Użyte w Procedurze definicje i skróty oznaczają:

- 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;
- dane osobowe – wszelkie 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;
- Użytkownik – osoba upoważniona do przetwarzania danych przez administratora danych;
- IOD – inspektor ochrony danych;
- ASI - administrator systemów informatycznych (Informatyk)
- RODO – Rozporządzenie Parlamentu Europejskiego i Rady (WE) 2016/679 z 27.04.2016r. 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. Urz. UE L 119/1 z 04.05.2016).

3. Naruszenie ochrony danych może być wynikiem:

- zdarzeń losowych (np. pożar, powódź, utrata zasilania, utrata łączności, wirus komputerowy, awarie komputerów, twardych dysków, oprogramowania itp.)
- umyślnych i nieumyślnych działań bądź zaniechań użytkowników.
- załącznik nr 3 zawiera przykładowe naruszenia oraz przykładowy katalog zagrożeń i podatności.

4. O możliwości zaistnienia przypadku naruszenia ochrony danych osobowych mogą świadczyć m.in.:

- nieprawidłowości w zakresie zabezpieczeń fizycznych miejsc przetwarzania i przechowywania danych osobowych, np. otwarte szafy, biurka, regały, niedomykające się okna;
- nieprawidłowości w pracy systemów informatycznych lub programów;
- nowe „podejrzane" konta użytkowników;
- maile zachęcające do ujawnienia identyfikatora i/lub zmiany hasła;

Zgłaszanie zdarzeń.

Niezależnie od źródła wykrycia zdarzenia naruszenia bezpieczeństwa każda osoba powiadomiona o tym fakcie lub taka, która sama zauważyła coś niezwykłego, jest odpowiedzialna za zainicjowanie dalszego postępowania i za poinformowanie o tym.

Poprawne zachowanie w przypadku takich zdarzeń obejmuje:

- obowiązek natychmiastowego zanotowania wszystkich ważnych szczegółów (np. typu niezgodności lub naruszenia, błędu działania, wiadomości z ekranu, dziwnego zachowania),
- zakaz podejmowania jakichkolwiek własnych działań i natychmiastowe zgłoszenie incydentu do punktu kontaktowego.

Sposób postępowania w przypadku podejrzenia naruszenia ochrony danych osobowych.

1. Każdy pracownik, który stwierdzi fakt naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe, bądź posiada informację mogącą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany niezwłocznie zgłosić to do ***IOD i do bezpośredniego przełożonego.***

2. Osoba zgłaszająca zdarzenie powinna udokumentować je opisując jak najwięcej dostępnych informacji ***(załącznik nr 1)***.

W opisie incydentu należy zamieścić takie istotne informacje jak:

- na czym polega incydent,
- data i godzina wystąpienia incydentu,
- imię i nazwisko oraz informacje kontaktowe (między innymi numer telefonu) zgłaszającego,
- jakiego systemu czy aplikacji dotyczy incydent,
- opis incydentu (np. kiedy wystąpił i czy jest powtarzalny, ewentualny wpływ incydentu na funkcjonowanie systemu)
- wstępne oszacowanie szkód, jeśli doszło do takowych,
- czy czynnik wywołujący incydent (na przykład intruz albo oprogramowanie złośliwe) został zidentyfikowany i czy jego aktywność nadal trwa,
- komunikaty jeśli są dostępne,

3. Do czasu uzyskania wskazówek lub poleceń od administratora lub osoby przez niego upoważnionej bądź IOD użytkownik powinien:

- przerwać przetwarzanie danych, w szczególności nie podejmować dalszej pracy w systemie informatycznym, a także podjąć inne czynności niezbędne do zapobieżenia skutkom zaistniałego naruszenia lub do ich ograniczenia;
- w miarę możliwości zabezpieczyć dowody świadczące o podejrzeniu lub naruszeniu ochrony danych;
- podjąć, stosownie do zaistniałej sytuacji, działania, które zapobiegną ewentualnej utracie danych osobowych;
- przekazać IOD lub swojemu bezpośredniemu przełożonemu informacje o miejscu, czasie, okolicznościach i możliwych przyczynach incydentu mogącego mieć lub mającego znamiona naruszenia ochrony danych.

3. W przypadku uzyskania informacji o podejrzeniu lub naruszeniu ochrony danych osobowych IOD zobowiązany jest niezwłocznie podjąć działania w celu ustalenia, czy zgłoszone zdarzenie miało miejsce, jakie były jego okoliczności i czy stanowiło naruszenie ochrony danych osobowych.

4. W przypadku stwierdzenia, że zdarzenie nie stanowi naruszenia ochrony danych, IOD dokumentuje wykonane czynności i podejmuje decyzję o możliwości dalszej pracy i przetwarzania danych przez Użytkowników, w tym w systemach informatycznych. Niezależnie od tego czy naruszenie zostanie zgłoszone do organu, fakt jego zaistnienia zostaje odnotowany w rejestrze naruszeń. ***(załącznik nr 2).***

5. W razie stwierdzenia naruszenia ochrony danych IOD zobowiązany jest:

- podjąć czynności w celu natychmiastowego usunięcia naruszenia i ograniczenia skutków naruszenia dla osób dotkniętych naruszeniem;
- wyjaśnić wszystkie okoliczności związane z naruszeniem, w tym czas, jego miejsce, zakres, a także źródło i osoby odpowiedzialne;
- zabezpieczyć dowody zdarzenia;
- umożliwić dalsze, bezpieczne przetwarzanie danych przez Użytkowników;
- oszacować ryzyko naruszenia praw i wolności osób fizycznych dotkniętych zdarzeniem bez zbędnej zwłoki, nie później jednak niż w terminie 48 godzin od stwierdzenia naruszenia i przekazać ocenę Administratorowi;
- udokumentować zaistniały przypadek naruszenia ochrony danych, sporządzając protokół ;
- wdrożyć działania naprawcze.

6. W przypadku naruszenia ochrony danych osobowych Administrator bez zbędnej zwłoki – w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza naruszenie Prezesowi UODO, chyba, że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych (art. 33 ust. 1 RODO).

7. Jeśli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator, bez zbędnej zwłoki, zawiadamiania osobę, której dane dotyczą, o takim naruszeniu, (art. 34 ust. 1 RODO).

8. IOD zobowiązany jest dokonać analizy sposobu poinformowania osób, które zostały dotknięte naruszeniem.

Sposób postępowania w przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego.

1. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego osoba stwierdzająca naruszenie obowiązana jest niezwłocznie powiadomić o tym ***administratora systemów informatycznych.***

2. Do czasu przybycia na miejsce naruszenia danych osobowych ASI lub innej upoważnionej osoby, należy:

- niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia (o ile istnieje taka możliwość) – a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców naruszenia danych osobowych;
- udokumentować wstępnie zaistniałe naruszenie ***(załącznik nr 1)***
- nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia ASI lub innej upoważnionej osoby.

3. ASI po otrzymaniu powiadomienia:

- podejmuje niezbędne działania mające na celu uniemożliwienie dalszego naruszenia zabezpieczenia systemu (odłączenie urządzeń, zmiana haseł),
- zabezpiecza, utrwala wszelkie informacje systemów i dokumenty, które mogą stanowić pomoc przy ustaleniu przyczyn naruszenia,
- ustala charakter i rodzaj naruszenia oraz metody działania osób naruszających zabezpieczenie systemu,
- niezwłocznie przywraca prawidłowy stan działania systemu, a w przypadku uszkodzenia baz danych odtwarza je z ostatnich kopii awaryjnych z zachowaniem należytych środków ostrożności,
- dokonuje analizy stanu systemu wraz z oszacowaniem rozmiaru szkód powstałych na skutek naruszenia,
- sporządza szczegółowy raport zawierający w szczególności: datę i godzinę otrzymania informacji o naruszeniu(włamania do systemu), opis jego przebiegu, przyczyny oraz wnioski ze zdarzenia.

4. Raport wraz z ewentualnymi załącznikami (np. kopie dowodów dokumentujących naruszenie) administrator systemów informatycznych przekazuje administratorowi danych lub/i inspektorowi danych osobowych.

5. ASI w porozumieniu z administratorem danych lub/i inspektorem danych osobowych podejmują niezbędne działania w celu zapobieżenia naruszeniom w przyszłości.

6. Administrator systemów informatycznych, w porozumieniu z administratorem danych osobowych lub inspektorem danych osobowych, podejmuje niezbędne działania w celu wyeliminowania naruszeń zabezpieczeń danych w przyszłości, a w szczególności:

- jeżeli przyczyną zdarzenia był stan techniczny urządzenia, sposób działania programu, uaktywnienie się wirusa komputerowego lub jakość komunikacji w sieci telekomunikacyjnej, niezwłocznie przeprowadza, w stosownym zakresie, przeglądy oraz konserwacje urządzeń i programów, ustala źródło pochodzenia wirusa oraz wdraża skuteczniejsze zabezpieczenia antywirusowe, a w miarę potrzeby kontaktuje się z dostawcą usług telekomunikacyjnych,
- jeżeli przyczyną zdarzenia były wadliwe metody pracy, błędy i zaniedbania osób zatrudnionych przy przetwarzaniu danych osobowych, przeprowadza dodatkowe kursy i szkolenia osób biorących udział przy przetwarzaniu danych, a wobec osób winnych zaniedbań wnioskuje do administratora danych o wyciągniecie konsekwencji prawem przewidzianych.

Postanowienia końcowe.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do zapoznania się z niniejsza instrukcją. Wykonanie powyższego zobowiązania pracownik potwierdza własnoręcznym podpisem.

2. Wszelkie zmiany niniejszej instrukcji skutkują wobec osób, których dotyczą z dniem ich doręczenia na piśmie.

Załącznik nr 1

Zgłoszenie naruszenia ochrony danych osobowych

Imię i nazwisko oraz informacje kontaktowe zgłaszającego
Data i godzina stwierdzenia naruszenia / incydentu
Lokalizacja zdarzenia (nr pokoju, nazwa pomieszczenia)
Jakiego systemu / aplikacji dotyczy?
Na czym polega naruszenie / incydent
Wstępne oszacowanie szkód, jeśli doszło do takowych
Komunikaty, jeśli są dostępne

Podpis pracownika	**Data i podpis IOD**

Załącznik nr 2

Rejestr naruszeń ochrony danych osobowych

Rodzaj naruszenia	Obowiązek zgłoszenia organowi nadzorczemu	Obowiązek zawiadomienia osoby, której dane dotyczą	Okoliczności naruszenia	Skutki naruszenia	Podjęte działania zaradcze

Załącznik nr 3

Przykłady naruszenia ochrony danych osobowych

1.	stwierdzono naruszenie zabezpieczenia systemu informatycznego lub urządzeń, nośników przetwarzających dane (laptop, telefon, pendrive, dysk zewnętrzny itp.)
2.	sposób działania programu lub jakość komunikacji w siec telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych,
3.	nieuprawnione ujawnienia danych osobowych,
4.	udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym,
5.	zabrania danych przez osobę nieupoważnioną,
6.	niewłaściwe zabezpieczenie fizyczne pomieszczeń lub dokumentacji,
7.	nieodpowiednie zabezpieczenie sprzętu IT czy oprogramowania,
8.	nieprawidłowe zaadresowanie korespondencji elektronicznej,
9.	nieautoryzowany dostęp do systemów informatycznych i urządzeń przetwarzających dane
10.	nieautoryzowane modyfikacje lub zniszczenie,
11.	pozyskiwanie informacji z nielegalnych źródeł
12.	nieupoważniony dostęp, modyfikację, kopiowanie lub zniszczenie/usunięcie danych osobowych
13.	pozostawiania danych w miejscu ogólnie dostępnym (np. na drukarkach, kopiarkach)
14.	zgubienie pendriva, laptopa lub innego nośnika,
15.	nieautoryzowany dostęp do danych przez połączenie sieciowe,
16.	dostęp do pomieszczeń, w których przetwarza się dane osobowe dla osób nieuprawnionych,
17.	niezablokowanie dostępu do systemu,
18.	brak nadzoru nad serwisantami i innymi osobami nieuprawnionymi przebywającymi w pomieszczeniach gdzie przetwarza się dane osobowe,
19.	wykrycie niezabezpieczonego kanału dystrybucji danych osobowych,
20.	nielegalne bądź nieświadome ujawnienie danych osobowych,
21.	pozyskiwanie danych osobowych z nielegalnych źródeł,
22.	przetwarzanie danych osobowych niezgodne z uprawnionym celem i zakresem,
23.	stwierdzenie obecności wirusów komputerowych lub innych programów godzących w integralność systemu informatycznego,
24.	ujawnienie indywidualnych haseł dostępu do systemu,
25.	przesyłanie danych osobowych przez Internet bez zabezpieczenia,
26.	niestosowanie zasady czystego biurka i czystego ekranu,
27.	przesyłanie dokumentów papierowych i nośników elektronicznych z danymi bez zabezpieczenia,
28.	wykonanie nieuprawnionych kopii danych osobowych,
29.	naruszenie bezpieczeństwa kopii danych osobowych,
30.	kradzież nośników zawierających dane osobowe,
31.	kradzież sprzętu służącego do przetwarzania danych osobowych,

32.	utratę danych osobowych w systemie informatycznym, na kopiach bezpieczeństwa i na innych nośnikach,
33.	brak aktualnych kopii bezpieczeństwa danych osobowych
34.	niewłaściwe niszczenie nośników z danymi osobowymi pozwalające na ich odczyt,
35.	naruszenie zasad ochrony fizycznej pomieszczeń, w których przetwarza się dane osobowe,
36.	dopuszczenie do przetwarzania danych osobowych pracowników bez odpowiednich upoważnień,
37.	nie zawarcie umowy powierzenia z firmami współpracującymi (serwis, naprawa i inne),
38.	przekazanie danych osobowych za pośrednictwem osób nieupoważnionych,

Katalog zagrożeń i podatności	
Działania celowe:	
Zagrożenia	**Podatności**
OPROGRAMOWANIE ZŁOŚLIWE	wirus - robak sieciowy - koń trojański
PRZEŁAMANIE ZABEZPIECZEŃ	nieuprawnione logowanie - naruszenie procedur - włamanie do aplikacji - włamanie na konto/ataki siłowe
PUBLIKACJE W SIECI INTERNET	naruszenie praw autorskich - pomawianie (zniesławianie) - treści obraźliwe
SABOTAŻ KOMPUTEROWY	podsłuch - skanowanie - dezinformacja - SPAM - szpiegostwo - atak odmowy dostępu
CZYNNIK LUDZKI	nieuprawniony dostęp lub nieuprawnione wykorzystanie informacji - nieuprawniona zmiana informacji - wykorzystanie podatności aplikacji - wykorzystanie podatności w urządzeniach - skasowanie danych
CYBERTERRORYZM	przestępstwo o charakterze terrorystycznym popełnione w cyberprzestrzeni
Działanie niecelowe:	
ZDARZENIA LOSOWE ZEWNĘTRZNE	pożar, zalanie wodą, utrata zasilania, utrata łączności
ZDARZENIA LOSOWE WEWNĘTRZNE	awarie sprzętowe - awarie łącza - awarie (błędy) oprogramowania
CZYNNIK LUDZKI :	brak wiedzy - zaniedbanie, naruszenie procedur