Dokument
podpisany przez
Piotr Kopijasz
Data: 2022.09.23
17:18:53 CEST

DYREKTOR
Wojewódzkiego Szpitala Psychiatrycznego
w Andrychowie
Piotr Kopijasz

do Zarządzenia Dyrektora WSP
nr 4/2019 z dnia 20.02.2019r.

Polityka Bezpieczeństwa
w zakresie ochrony danych osobowych
w Wojewódzkim Szpitalu Psychiatrycznym
w Andrychowie

CZĘŚĆ A.

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 w Wojewódzkim Szpitalu Psychiatrycznym w Andrychowie.

Niniejszy dokument został opracowany zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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 (Dz.U. 1998.21.94 – tekst jednolity z późn. zm.) oraz przepisów wykonawczych z nim związanych*,
3) przepisów ustawy z dnia 15 kwietnia 2011r. *o działalności leczniczej (Dz.U.2011.112.654) oraz przepisów wykonawczych z nią związanych,*
4) przepisów ustawy z dnia 19 sierpnia 1994r. *o ochronie zdrowia psychicznego (Dz.U.2004.111.535 z późn. zm) oraz przepisów wykonawczych z nią związanych*,
5) przepisów ustawy z dnia 26 października 1982r. *o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi (Dz.U.1982.35.230 – tekst jednolity z późn.zm.) oraz przepisów wykonawczych z nią związanych,*
6) przepisów ustawy z dnia 29 lipca 2005r. *o przeciwdziałaniu narkomanii (Dz.U.2005.179.1485 z późn. zm.) oraz przepisów wykonawczych z nią związanych,*
7) przepisów ustawy z dnia 5 grudnia 1996r. *o zawodach lekarza i lekarza dentysty (Dz.U.1997.28.152 – tekst jednolity z późn. zm.) oraz przepisów wykonawczych z nią związanych,*
8) przepisów ustawy z dnia 5 lipca 1996r. *o zawodach pielęgniarki i położnej (Dz.U.2011.174.1039 – tekst jednolity z późn. zm.) oraz przepisów wykonawczych z nią związanych,*
9) przepisów ustawy z dnia 6 listopada 2008r. *o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U.2009.52.417 z późn. zm.) 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.2008.234.1570 z późn. zm) oraz przepisów wykonawczych z nią związanych,*
11) przepisów ustawy z dnia 27 sierpnia 2004r. *o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz.U.2004.210.2135 – tekst jednolity z późn. zm.) oraz przepisów wykonawczych z nią związanych,*
12) przepisów ustawy z dnia 22 maja 2003r. *o działalności ubezpieczeniowej (Dz.U.2010.11.66 – tekst jednolity z późn. zm.) 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.2015.poz2069),*

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,*
- ✓ *Regulamin użytkowania komputerów przenośnych oraz zewnętrznych nośników danych*

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 kwietnia 2016 r. (Dz. Urz. UE L 119 z 4 maja 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.

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 i 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.

Rozdział 2.

Katalog zagrożeń i incydentów naruszających ochronę danych osobowych

1. Rodzaje zagrożeń naruszających ochronę danych osobowych:

- ✓ zagrożenia losowe:
  a) 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,
  b) 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:
  a. nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
  b. nieuprawniony dostęp do systemu z jego wnętrza,
  c. nieuprawniony przekaz danych,
  d. 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.).

3. 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 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, taśmach magnetycznych, 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. Osoby nieupoważnione do przetwarzania danych osobowych określonej kategorii, mające interes prawny lub faktyczny w uzyskaniu dostępu do tych danych lub wykonujące inne czynności nie mające związku z dostępem do tych danych mogą przebywać w pomieszczeniach tworzących obszar, w którym przetwarzane są dane osobowe wyłącznie w obecności upoważnionego pracownika.
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 nadawane są do zbiorów na wniosek przełożonych osób. Upoważnienia określają zakres operacji na danych, np. tworzenie, usuwanie, wgląd, przekazywanie.
6. Upoważnienia mogą być nadawane w formie poleceń, np. upoważnienia do przeprowadzenia kontroli, wykonania czynności służbowych, udokumentowanego polecenia Administratora w postaci umowy powierzenia
7. Administrator/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.***
8. Wzór upoważnienia zawarty jest w ***załączniku nr 4*** do niniejszej Polityki bezpieczeństwa.
9. Szczegółowa instrukcja nadawania upoważnienia 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 6.***

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:

A) Procedura nadawania/zmiany/odwołania upoważnień do przetwarzania danych.
B) Opis zastosowanych zabezpieczeń technicznych.
C) Opis zastosowanych zabezpieczeń organizacyjnych.
D) Procedura postępowania przy naruszeniu bezpieczeństwa danych
E) Zasady udostępniania danych.
F) Procedury powierzania danych.
G) Obowiązki ASI
H) Obowiązki IOD

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

B. Opis zastosowanych zabezpieczeń technicznych:

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

- ✓ 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,

C. Opis zastosowanych zabezpieczeń organizacyjnych:

- ✓ opracowano i wdrożono politykę bezpieczeństwa dla pracowników zatrudnionych przy przetwarzaniu danych osobowych,
- ✓ opracowano i wdrożono instrukcję zarządzania systemem informatycznym,
- ✓ 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.

D. Procedura postępowania przy naruszeniu bezpieczeństwa danych

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 ***„Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych”***, która stanowi integralną część do Polityki bezpieczeństwa.

„Instrukcja ….” 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 wg wzoru stanowiącego ***Załącznik Nr 7***, który powinien zawierać w szczególności:
- wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
- określenie czasu, miejsca naruszenia i powiadomienia,
- określenie okoliczności towarzyszących i rodzaju naruszenia,
- opis podjętego działania,
- wstępną ocenę przyczyn wystąpienia naruszenia,
- ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

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.

E. 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.

F. 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.

G. 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*.

H. 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 (***załącznik nr 8*** do „Polityki bezpieczeństwa").
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 podjęcia Uchwały Zarządu organizacji lub w terminie określonym w treści tej Uchwały.
8. Zmiany w „Polityce bezpieczeństwa" będą wchodzić w życie w terminach określonych w Uchwałach Zarządu organizacji dotyczących wprowadzenia zmian w dokumencie.

Załącznik nr 1
do „Polityki bezpieczeństwa
w zakresie ochrony danych osobowych
w WSP w Andrychowie” z dnia 20.02.2019r.

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

Lp.	Komórka organizacyjna przetwarzająca dane osobowe w systemie informatycznym	Pomieszczenie, w którym przetwarzane są dane osobowe
1	Główny Księgowy	pok. A-305, II piętro budynek segment „A”
2	Dział Finansowo-Księgowy	Pok. A-302, II piętro budynek segment „A”
3	Kasa	pok. A-301, II piętro budynek segment „A”
4	Dział Kadr i Organizacji Pracy	pok. A -308, A-309, II piętro budynek segment „A”
5	Przełożona Pielęgniarek	pok. A-304, II piętro budynek segment „A”
6	Sekretariat	Pok. A-306, II piętro budynek segment „A”
7	Dział Zamówień Publicznych	pok. A-303, II piętro budynek segment „A”
8	Pielęgniarka epidemiologiczna Pracownik socjalny	pok. A-310, II piętro budynek segment „A”
9	BHP - Serwer	pok. A-206, I piętro budynek segment „A”
10	Pracownia Diagnostyki Laboratoryjnej	pok. A-201, I piętro budynek segment „A”
11	Dział Techniczno-Eksploatacyjny	pok. A-113, pok. A-114, parter budynek segment „A”
12	Oddział dzienny terapii uzależnień bliżej niescharekteryzowanych	Pok 1,2,3 - Gabinety terapeutów parter budynek segment „A”
13	Poradnia terapii uzależnienia od alkoholu i współuzależnienia	
14	Dział Statystyki i Zarządzania Informacją	pok. C-108, parter budynek segment „C”
15	Izba przyjęć	pok. C-118, parter budynek segment „C”
16	Poradnia Zdrowia Psychicznego	pok. C-126, parter budynek segment „C”
17	Oddział psychiatryczny I	Gabinet lekarski, parter Sekretariat oddziału, parter Gabinet lekarski, I parter budynek segment „B”
18	Oddział psychiatryczny II	Sekretariat oddziału, I piętro

		Gabinet Ordynatora, I piętro budynek segment „D”
19	Oddział psychiatryczny III	Gabinet pielęgniarki oddziałowej, II piętro budynek segment „B”
20	Oddział dzienny psychiatryczny	Gabinet terapeutów, 1 piętro budynek segment „D”
21	Oddział psychogeriatryczny	Sekretariat oddziału, parter budynek segment „D”
22	Oddział leczenia alkoholowych zespołów abstynencyjnych	Sekretariat oddziału, parter Gabinety lekarskie, parter budynek segment „D”
23	Oddział terapii uzależnienia od alkoholu	pok. 1.2, Sekretariat oddziału, parter pok. 1.3 Gabinet Lekarski, parter pok. 1.37 Kierownik zespołu terapeutycznego, parter Gabinet Lekarski, I piętro budynek segment „F”

Załącznik nr 2
do „Polityki bezpieczeństwa
w zakresie ochrony danych osobowych
w WSP w Andrychowie” z dnia 20.02.2019r.

Wykaz zbiorów danych osobowych i programów zastosowanych do ich przetwarzania w Wojewódzkim Szpitalu Psychiatrycznym w Andrychowie

Lp.	Zbiory danych osobowych	Nazwa bazy danych	Wersja bazy danych	Forma bazy danych/System operacyjny serwera	Sposób zabezpieczenia informatycznego	Baza danych chroniona przez UPS (Tak/Nie)	Liczba miejsc przetwarzania
1	FK/Koszty	ADM	11	ORACLE	Hasło	Tak	2
2	Kadry Płace	ADM	11	ORACLE	Hasło	Tak	4
3	Płatnik	WSP		MDB	Hasło	Tak	2
4	Pracownicy	BHP		UDB	Hasło	Tak	1
5	Pacjenci	SZP	11	ORACLE	Hasło	Tak	7
6	Pacjenci	RUCH		DBASE	Hasło	Tak	4

Załącznik nr 3
do „Polityki bezpieczeństwa
w zakresie ochrony danych osobowych
w WSP w Andrychowie” z dnia 20.02.2019r.

WZÓR

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
do „Polityki bezpieczeństwa
w zakresie ochrony danych osobowych
w WSP w Andrychowie" z dnia 20.02.2019r.

WZÓR

Upoważnienie nr
do przetwarzania danych osobowych

- ✓ Na podstawie art. 29 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 swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych) upoważniam Panią/Pana **……..** zatrudnioną/nego na podstawie umowy o pracę na stanowisku **……..** w Wojewódzkim Szpitalu Psychiatrycznym w Andrychowie do przetwarzania danych osobowych w systemie informatycznym* / wersji papierowej*.
- ✓ Upoważnienie obejmuje przetwarzanie danych osobowych na wyznaczonym stanowisku pracy, zgodnie z powierzonymi obowiązkami pracowniczymi oraz poleceniami służbowymi.
- ✓ Identyfikator: ……

  (wypełnia się w przypadku, gdy dane przetwarzane są w systemie informatycznym)
- ✓ Jednocześnie zobowiązuję Panią/Pana do zachowania w tajemnicy (również po ustaniu stosunku zatrudnienia) danych osobowych uzyskanych w trakcie dokonywania operacji związanych z ich przetwarzaniem oraz sposobów ich zabezpieczania.
- ✓ 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)

- niniejsze upoważnienie zostało sporządzone w trzech jednobrzmiących egzemplarzach, które otrzymują:
1. Osoba upoważniona.
2. Dział Kadr i Organizacji Pracy – do akt osobowych upoważnionego.
3. a/a

***)niepotrzebne skreślić**

Załącznik nr 5
do „Polityki bezpieczeństwa
w zakresie ochrony danych osobowych
w WSP w Andrychowie" z dnia 20.02.2019r.

WZÓR

Odwołanie upoważnienia nr
do przetwarzania danych osobowych

Z dniem …….. na podstawie *art. 24 ust. 1 i art. 32 ust. 4 w związku z art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE* odwołuję Pani/Panu …….upoważnienie do przetwarzania danych osobowych nr ……. nadane ……..

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

- niniejsze odwołanie upoważnienia zostało sporządzone w trzech jednobrzmiących egzemplarzach, które otrzymują:
1. Osoba upoważniona
2. Dział Kadr i Organizacji Pracy – do akt osobowych pracownika.
3. a/a

Załącznik nr 6
do „Polityki bezpieczeństwa
w zakresie ochrony danych osobowych
w WSP w Andrychowie” z dnia 20.02.2019r.

Struktura zbiorów danych osobowych przetwarzanych w systemie informatycznym oraz sposób ich przepływu w Wojewódzkim Szpitalu Psychiatrycznym w Andrychowie

L.p.	Nazwa bazy danych	Zbiór danych osobowych	Zawartość poszczególnych pól informacyjnych i powiązania między nimi	Sposób przepływu danych
1	ADM	FK/Koszty	**Zakres:** Imię i nazwisko, adres zamieszkania, data i miejsce urodzenia, nr konta bankowego	Brak przepływu danych
2	ADM	Kadry Płace	**Zakres:** Imię i nazwisko, dane adresowe, dane o wykształceniu, przebiegu pracy, absencji, zakres obowiązków, stawki wynagrodzenia, kary, nagrody	Ewidencja papierowa > program Kadry Płace > Bank
3	WSP	Płatnik	**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
4	BHP	Pracownicy	**Zakres:** Imię i nazwisko, data zatrudnienia, data i miejsce urodzenia, miejsce zamieszkania	Brak przepływu danych
5	SZP	Pacjenci	**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
6	RUCH	Pacjenci	**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	Brak przepływu danych

Załącznik nr 7
do „Polityki bezpieczeństwa
w zakresie ochrony danych osobowych
w WSP w Andrychowie" z dnia 20.02.2019r.

WZÓR

Raport
z naruszenia bezpieczeństwa danych osobowych

- ✓ Data: ……..… Godzina ……
  (dd.mm.rrrr) (gg:mm)
- ✓ Osoba powiadamiająca o zaistniałym zdarzeniu:
  ……...
  (imię, nazwisko, stanowisko służbowe, nazwa użytkownika)
- ✓ Lokalizacja zdarzenia:
  ……
  (np. nr pokoju, nazwa pomieszczenia)
- ✓ Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu:

……
……
……

- ✓ Przyczyny wystąpienia zdarzenia:

……
……
……

- ✓ Postępowanie wyjaśniające i naprawcze:
  ……
  ……
  ……

…….

(Data , pieczątka i podpis Dyrektora Szpitala)

Załącznik nr 8
do „Polityki bezpieczeństwa
w zakresie ochrony danych osobowych
w WSP w Andrychowie" z dnia 20.02.2019r.

WZÓR

Oświadczenie w sprawie zaznajomienia z przepisami dotyczącymi ochrony danych osobowych

✓ Ja, niżej podpisana(y) **……**

(imię i nazwisko)

jako pracownik Wojewódzkiego Szpitala Psychiatrycznego w Andrychowie, zatrudniona(y) na stanowisku ……..

(stanowisko służbowe)

wiążącym się z wykonywaniem pracy przy przetwarzaniu danych osobowych oświadczam, że zostałam (em) zaznajomiona (y) z przepisami 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 swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych) oraz obowiązującą w jednostce:

- polityką bezpieczeństwa w zakresie ochrony danych osobowych,
- instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
- instrukcją postępowania w sytuacji naruszenia systemu ochrony danych osobowych.
- regulaminem użytkowania komputerów przenośnych oraz zewnętrznych nośników dysku.

✓ Zobowiązuje się:

- zachować w tajemnicy dane osobowe, do których mam dostęp w związku z zajmowanym stanowiskiem oraz sposoby ich zabezpieczenia,
- chronić dane osobowe przed dostępem do nich osób do tego nieupoważnionych.

……..
(data i podpis pracownika)

- niniejsze oświadczenie zostało sporządzone w trzech jednobrzmiących egzemplarzach, które otrzymują:
1. Osoba upoważniona
2. Dział Kadr i Organizacji Pracy – do akt osobowych pracownika.
3. a/a

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

CZĘŚĆ B.

CZĘŚĆ B	**Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Wojewódzkim Szpitalu Psychiatrycznym w Andrychowie**	
Spis treści		33
Rozdział 1	Wprowadzenie	34
Rozdział 2	Procedury nadawania uprawnień do przetwarzania danych osobowych i rejestrowanie tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności	35
Rozdział 3	Stosowane metody i środki uwierzytelniania oraz procedury związane zarządzaniem nimi i ich użytkowaniem	36
Rozdział 4	Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu	37
Rozdział 5	Procedury tworzenia kopii zapasowych, zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania	39
Rozdział 6	Sposób, miejsce i okres przechowywania wydruków, elektronicznych nośników informacji oraz kopii zapasowych zawierających dane osobowe	39
Rozdział 7	Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego	40
Rozdział 8	Udostępnianie danych osobowych i sposób odnotowania informacji o udostępnionych danych	41
Rozdział 9	Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji do przetwarzania danych	42
Rozdział 10	Ustalenia końcowe	43

Rozdział 1.

Wprowadzenie

1. Podstawę prawną dla opracowania i wdrożenia niniejszej instrukcji stanowią:

- ✓ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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).

2. Instrukcja zarządzania 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 przy przetwarzaniu danych osobowych w systemach informatycznych.
3. Instrukcja określa zasady i procedury zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
4. Wszystkie osoby zatrudnione przy przetwarzaniu danych osobowych w systemach informatycznych bez względu na zajmowane stanowisko i miejsce pracy oraz charakter stosunku pracy są zobowiązane do postępowania zgodnie z zasadami określonymi w niniejszej instrukcji.
5. Nieprzestrzeganie postanowień niniejszej instrukcji oraz brak nadzoru nad bezpieczeństwem informacji stanowi naruszenie obowiązków pracowniczych podlegających sankcjom dyscyplinarnym oraz sankcjom karnym.
6. 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, może być dopuszczona wyłącznie osoba posiadająca upoważnienia do przetwarzania 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.
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 nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego, nie powinien być przydzielany innej osobie.
7. Użytkownikom nadawane są uprawnienia do pracy tylko w wymaganych dla realizacji powierzonych zadań modułach i funkcjach programów. Przyznanie, zmiana lub ograniczenie uprawnień następuje na pisemny wniosek przełożonego użytkownika złożony administratorowi danych.
8. Administrator danych informuje administratora systemu informatycznego o fakcie ograniczenia lub utraty przez daną osobę uprawnień do dostępu do danych osobowych w systemie informatycznym. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych, należy niezwłocznie wyrejestrować z systemu informatycznego, unieważnić jej hasło, oraz podjąć inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych.
9. Za realizację procedury rejestrowania i wyrejestrowania użytkowników w systemie informatycznym odpowiedzialny jest administrator systemu informatycznego.

10. 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.

Służbowa poczta elektroniczna

11. Pracownik powinien zabezpieczyć dostęp do służbowej poczty elektronicznej (służbowego adresu e-mail) poprzez nadanie jej indywidualnego hasła ochronnego.
12. Pierwsze hasło jest nadawane Pracownikowi przez Administratora Systemów Informatycznych.
13. Pracownik jest zobowiązany do zmiany hasła podczas pierwszego logowania się do służbowej poczty elektronicznej.
14. Pracownik powinien chronić hasło przed dostępem osób trzecich. W każdym przypadku, gdy hasło zostało ujawnione innej osobie, Pracownik jest zobowiązany do jego zmiany.
15. Pracownik powinien wykorzystywać służbową pocztę elektroniczną (służbowy adres e- mail) jedynie do czynności związanych z wykonywaną pracą.
16. Zabronione jest wykorzystywanie prywatnej poczty elektronicznej (prywatnego adresu e-mail) do celów służbowych.
17. Przyznanie służbowego adresu e-mail następuje na pisemny wniosek przełożonego użytkownika złożony administratorowi danych.
18. Pracownik jest zobowiązany do korzystania z przyznanego mu adresu mailowego do wszelkiej korespondencji służbowej z innymi pracownikami placówki.
19. 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;
    - podawania tematu e-mail'a oraz umieszczania swojego podpisu.
20. 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.
21. 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.
22. 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. 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.
2. Kopie zapasowe są tworzone, przechowywane i wykorzystywane z uwzględnieniem następujących zasad:
   - wykonywane są codziennie,
   - wykonywane są przez kopiowanie całości danych,
   - po wykonaniu kopii zapasowej i awaryjnej administrator systemu informatycznego ma obowiązek sprawdzić poprawność i kompletność skopiowanych danych,
   - kopie zapasowe są okresowo sprawdzane pod kątem ich przydatności do odtworzenia w przypadku awarii systemu.
3. Za sporządzanie i bezpieczeństwo kopii zapasowych i awaryjnych odpowiedzialny jest administrator systemu informatycznego.

Rozdział 6.

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

1. Wydruki archiwalne lub bieżące należy przechowywać w szafach zamykanych na klucz w pomieszczeniach 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 powinny być przechowywane 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. Nośniki danych po ustaniu ich użyteczności należy pozbawić danych lub zniszczyć 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 oraz oprogramowania złośliwego, 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:

- ✓ system informatyczny jest zabezpieczany przez zastosowanie rozwiązań sprzętowych i programowych,
- ✓ za aktualność stosowanych zabezpieczeń, dostosowywanie do aktualnych potrzeb, konfigurację i zarządzanie nimi odpowiada administrator systemu informatycznego,

- ✓ administrator systemu informatycznego ma obowiązek zgłaszać na piśmie administratorowi danych wszelkie potrzeby lub zauważone niedociągnięcia w zakresie zapewnienia bezpieczeństwa systemu informatycznego,
- ✓ w przypadku, gdy system zabezpieczeń wskazuje zaistnienie zagrożenia, użytkownicy są zobowiązani bezzwłocznie powiadomić o tym fakcie administratora systemu informatycznego, który po jego usunięciu sprawdza system i przywraca go do pełnej funkcjonalności,
- ✓ bezwzględnie zakazuje się użytkownikom samowolnego korzystania z prywatnych lub pochodzących ze źródła innego niż miejsce pracy nośników informacji. Korzystanie z takich nośników może mieć miejsce wyłącznie po uzyskaniu zgody administratora systemu informatycznego, po uprzednim sprawdzeniu nośnika informacji pod względem bezpieczeństwa dla systemu informatycznego,
- ✓ bezwzględnie zakazuje się użytkownikom wykorzystywania powierzonego im sprzętu informatycznego, oprogramowania i dostępu do zasobów informatycznych do jakichkolwiek celów innych niż wykonywanie powierzonych im czynności służbowych,
- ✓ bezwzględnie zakazuje się użytkownikom samowolnego instalowania na stacjach roboczych jakiegokolwiek oprogramowania z jakiegokolwiek źródła, za wyjątkiem aktualizowanych automatycznie komponentów systemu operacyjnego,
- ✓ bezwzględnie zabrania się użytkownikom łamania lub obchodzenia zabezpieczeń systemu informatycznego. O każdym przypadku znalezienia luki w zabezpieczeniach użytkownik ma obowiązek powiadomić administratora systemu informatycznego,
- ✓ użytkownicy są bezpośrednio odpowiedzialni za zainstalowane na powierzonych im stacjach roboczych oprogramowanie oraz mają obowiązek zgłaszać wszelkie wątpliwości w tym zakresie administratorowi systemu informatycznego, ze szczególnym uwzględnieniem zmian, które zostały wprowadzone podczas ich nieobecności.

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.

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:

2) wyrzucania zbędnych dokumentów zawierających dane osobowe bez uprzedniego ich trwałego zniszczenia,
3) pozostawiania dokumentów, kopii dokumentów zawierających dane osobowe w drukarkach, kserokopiarkach itd.
4) pozostawiania kluczy w drzwiach, szafach, biurkach, zostawiania otwartych pomieszczeń, w których przetwarza się dane osobowe,
5) pozostawiania bez nadzoru osób trzecich przebywających w pomieszczeniach, w których przetwarzane są dane osobowe,

6) pozostawiania dokumentów na biurku po zakończeniu pracy, pozostawiania otwartych dokumentów na ekranie monitora,
7) ignorowania nieznanych osób z zewnątrz poruszających się w obszarze przetwarzania danych osobowych,
8) przekazywania informacji będącymi danymi osobowymi osobom nieupoważnionym.

Konieczne jest:

9) posługiwanie się własnym hasłem w celu uzyskania dostępu do systemu informatycznego,
10) tworzenie haseł trudnych do odgadnięcia dla innych,
11) nie przerywanie procesu skanowania przez program antywirusowy na komputerze,
12) wykonywanie kopii zapasowych danych przetwarzanych na stanowisku komputerowym,
13) 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.

Instrukcja postępowania w sytuacji naruszenia systemu ochrony danych osobowych

CZĘŚĆ C.

Rozdział 1.

Postępowania ogólne.

- ✓ Instrukcja niniejsza określa tryb i zasady postępowania osób zatrudnionych przy przetwarzaniu danych osobowych, w przypadku gdy:
- ✓ 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
- ✓ Osobą odpowiedzialną za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie, jest administrator systemów informatycznych.

Rozdział 2.

Zgłaszanie zdarzeń.

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 o tym.

Osoba zgłaszająca zdarzenie powinna udokumentować je opisując jak najwięcej dostępnych informacji.

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,

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.

Rozdział 3.

Tryb postępowania w przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego.

- ✓ W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego osoba stwierdzająca naruszenie obowiązana jest niezwłocznie powiadomić o tym administratora systemów informatycznych.
- ✓ Do czasu przybycia na miejsce naruszenia danych osobowych ASI lub innej upoważnionej osoby, należy:

I) 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;

J) udokumentować wstępnie zaistniałe naruszenie – ***patrz rozdział 2.***

K) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia ASI lub innej upoważnionej osoby.

- ✓ Administrator systemów informatycznych po otrzymaniu powiadomienia:

8. podejmuje niezbędne działania mające na celu uniemożliwienie dalszego naruszenia zabezpieczenia systemu (odłączenie urządzeń, zmiana haseł),
9. zabezpiecza, utrwala wszelkie informacje systemów i dokumenty, które mogą stanowić pomoc przy ustaleniu przyczyn naruszenia,
10. ustala charakter i rodzaj naruszenia oraz metody działania osób naruszających zabezpieczenie systemu,

11. niezwłocznie przywraca prawidłowy stan działania systemu, a w przypadku uszkodzenia baz danych odtwarza je z ostatnich kopii awaryjnych z zachowaniem należytych środków ostrożności,
12. dokonuje analizy stanu systemu wraz z oszacowaniem rozmiaru szkód powstałych na skutek naruszenia,
13. sporządza szczegółowy raport zawierający w szczególności: datę i godzinę otrzymania informacji o naruszeniu(włamania do systemu), opis jego przebiegu, przyczyny oraz wnioski ze zdarzenia.

- ✓ Raport wraz z ewentualnymi załącznikami (np. kopie dowodów dokumentujących naruszenie) administrator systemów informatycznych przekazuje administratorowi danych lub/i inspektorowi danych osobowych.
- ✓ Administrator systemów informatycznych w porozumieniu z administratorem danych lub/i inspektorem danych osobowych podejmują niezbędne działania w celu zapobieżenia naruszeniom w przyszłości.

Rozdział 4.

Tryb postępowania w przypadku podejrzenia naruszenia zabezpieczeń danych osobowych.

- ✓ Każda osoba przetwarzająca dane osobowe, w przypadku podejrzenia naruszenia zabezpieczeń danych osobowych, obowiązana jest niezwłocznie powiadomić o tym administratora systemów informatycznych i/lub Inspektora danych osobowych.
- ✓ Stosownie do przypuszczalnego rodzaju naruszeń Administrator systemów informatycznych :

II. sprawdza stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
III. sprawdza sposób działania programu (w tym również obecność wirusów komputerowych),
IV. sprawdza jakość komunikacji w sieci telekomunikacyjnej,
V. sprawdza zawartość zbioru danych osobowych,
VI. poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych.

- ✓ W przypadku stwierdzenia naruszenia zabezpieczeń danych:
- ✓ podejmuje niezbędne działania mające na celu uniemożliwienie dalszego ich naruszenia (odłączenie wadliwych urządzeń, blokuje dostęp do sieci telekomunikacyjnej, do programów oraz zbiorów danych itp.),
- ✓ zabezpiecza, utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia,
- ✓ niezwłocznie przywraca prawidłowy stan działania systemu,
- ✓ dokonuje analizy stanu zabezpieczeń wraz z oszacowaniem rozmiaru szkód powstałych na skutek ich naruszenia,
- ✓ sporządza szczegółowy raport zawierający w szczególności: datę i godzinę otrzymania informacji o naruszeniu, opis jego przebiegu, przyczyny oraz wnioski ze zdarzenia.
- ✓ Raport, wraz z ewentualnymi załącznikami (kopie dowodów dokumentujących naruszenie), administrator systemów informatycznych przekazuje administratorowi danych lub/i inspektorowi danych osobowych.
- ✓ 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:

8. 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,
9. 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.

Rozdział 5.

Postanowienia końcowe.

14) Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do zapoznania się z niniejsza instrukcją. Wykonanie powyższego zobowiązania pracownik potwierdza własnoręcznym podpisem.
15) Wszelkie zmiany niniejszej instrukcji skutkują wobec osób, których dotyczą z dniem ich doręczenia na piśmie.

Regulamin użytkowania komputerów przenośnych oraz zewnętrznych nośników danych

CZĘŚĆ D.

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.