

POLITYKA BEZPIECZEŃSTWA INFORMACJI
I
INSTRUKCJA ZARZĄDZANIA
SYSTEMEM INFORMATYCZNYM W
SZPITALU SPECJALISTYCZNYM IM. J. DIETLA
W KRAKOWIE

Kraków, maj 2018 r.

ROZDZIAŁ I

POSTANOWIENIA OGÓLNE

§ 1

1. Podstawę prawną niniejszych unormowań stanowią:
 - 1) RODO - Rozporządzenie 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
 - 2) Ustawa o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz. U. z 2018 r. poz. 1000)
 - 3) inne akty prawne dotyczące działalności zakładów opieki zdrowotnej.
2. Ilekroć dalej jest mowa o:
 - 1) *danych osobowych* – należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, tj. osoby której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne,
 - 2) *zakładzie* – należy przez to rozumieć Szpital Specjalistyczny im. J. Dietla w Krakowie,
 - 3) *Administratorze Danych* – należy przez to rozumieć Szpital Specjalistyczny im. J. Dietla w Krakowie, w którego imieniu zadania w zakresie ochrony danych osobowych wykonuje Dyrektor zakładu, decydując o celach i środkach przetwarzania danych osobowych w zakładzie,
 - 4) *Pełnomocniku ds. Administrowania Danymi Osobowymi – Inspektor Ochrony Danych Osobowych* – należy przez to rozumieć pracownika wyznaczonego zarządzeniem Dyrektora zakładu lub na podstawie umowy o pracę, wykonującego powierzone przez Dyrektora obowiązki Administratora Danych Osobowych,
 - 5) *Administratorze Systemu Informatycznego (ASI)* – należy przez to rozumieć kierownika Sekcji Informatyki zakładu upoważnionego przez Pełnomocnika ds. Administrowania Danymi Osobowymi-Administratora Bezpieczeństwa Informacji do administrowania systemem informatycznym zakładu, przetwarzającym elektronicznie dane osobowe, który za pośrednictwem podległej mu Sekcji, zapewnia sprawne funkcjonowanie tego systemu,
 - 6) *Lokalnym Administratorze Systemu Informatycznego (LASI)* – należy przez to rozumieć osobę wyznaczoną przez Pełnomocnika ds. Administrowania Danymi Osobowymi-Administratora Bezpieczeństwa Informacji lub Administratora Systemu Informatycznego do administrowania wydzielonym systemem informatycznym przetwarzającym dane osobowe na wyznaczonym obszarze działania,
 - 7) *użytkownika* – należy przez to rozumieć osobę wykonującą zadania na rzecz zakładu, upoważnioną przez Pełnomocnika ds. Administrowania Danymi Osobowymi-Inspektora Ochrony Danych Osobowych do przetwarzania danych osobowych na wyznaczonym obszarze działania w zakresie wskazanym w upoważnieniu i wpisanego do ewidencji osób upoważnionych do przetwarzania danych osobowych,
 - 8) *użytkownika systemu informatycznego* – należy przez to rozumieć użytkownika posiadającego dostęp do ściśle określonego systemu informatycznego powierzony przez Administratora Systemu Informatycznego,
 - 9) *przetwarzaniu danych osobowych* – należy przez to rozumieć jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywa-

- nie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemie informatycznym,
- 10) *systemie informatycznym* – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu ochrony danych osobowych w zakładzie zgromadzonych w systemie elektronicznym,
 - 11) *zabezpieczaniu danych osobowych* – należy przez to rozumieć wdrażanie i eksploatację stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych osobowych w zakładzie, zgromadzonych w systemie elektronicznym i tradycyjnym,
 - 12) *bezpieczeństwie systemu informatycznego* – należy przez to rozumieć wszelkie działania służące zapewnieniu poufności tego systemu, dostępności do niego oraz jego integralności przy zastosowaniu środków technicznych i organizacyjnych,
 - 13) *obszarze przetwarzania danych osobowych* – należy przez to rozumieć budynki, pomieszczenia lub części pomieszczeń zakładu, w których są przetwarzane dane osobowe zarówno w formie tradycyjnej papierowej oraz elektronicznej, obejmujące miejsca, gdzie wykonuje się operacje na danych osobowych, jak również przechowuje się wszelkie nośniki informacji zawierające dane osobowe,
 - 14) *zbiorze danych osobowych* – należy przez to rozumieć każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie,
 - 15) *identyfikatorze użytkownika* – należy przez to rozumieć ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
 - 16) *hasło* – należy przez to rozumieć ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do przetwarzania danych osobowych w systemie informatycznym
 - 17) *prawie dostępu do zasobów informatycznych* – należy przez to rozumieć pisemne upoważnienie wydane użytkownikowi systemu informatycznego uprawniające do dostępu do tego systemu i przetwarzania danych osobowych i w wyznaczonym obszarze działania,
 - 18) *rozliczalności* – należy przez to rozumieć właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko jednemu podmiotowi,
 - 19) *poufności danych* – należy przez to rozumieć właściwość (czego ?) zapewniającą, że dane osobowe nie są udostępniane nieupoważnionym podmiotom,
 - 20) *sieci LAN/WAN* – należy przez to rozumieć sieć lokalną/rozległą umożliwiającą pracę systemu informatycznego przy wykorzystaniu specjalistycznych, dedykowanych urządzeń i sieci telekomunikacyjnych w rozumieniu ustawy z dnia 16.07.2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z póź. zm.), -
 - 21) *rejestrze udostępnionych danych osobowych* – należy przez to rozumieć rejestr, w którym odnotowywane są informacje o odbiorcach danych z systemu/aplikacji, prowadzonym dla danego systemu/aplikacji.
 - 22) *Monitoring wizyjny*- zespół współpracujących urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych do przetwarzania danych.
 - 23) *elektroniczna karta dostępu* – należy przez to rozumieć elektroniczną kartę dostępu (lub inny element dostępowy np. w formie breloka) stanowią dane zapisane w formie elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby przebywającej w obszarze przetwarzania danych osobowych na terenie zakładu.

ROZDZIAŁ II

POLITYKA BEZPIECZEŃSTWA W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH W ZAKŁADZIE

§ 2

1. Celem polityki bezpieczeństwa jest określenie działań, jakie należy podejmować oraz ustanowienie zasad, praw, reguł, procedur i praktycznych doświadczeń regulujących sposób przetwarzania, zarządzania, ochrony i dystrybucji danych osobowych wewnątrz zakładu i kontaktach z otoczeniem oraz sposobu zabezpieczania tych danych w zakładzie.
2. Polityka bezpieczeństwa zawiera:
 - 1) wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe,
 - 2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
 - 3) Rejestr czynności przetwarzania danych osobowych,
 - 4) Rejestr kategorii czynności przetwarzania
 - 5) Ocena skutków dla ochrony danych - cena ryzyka przetwarzania danych osobowych,
 - 6) określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych,
 - 7) Instrukcja naruszenia bezpieczeństwa informacji,
 - 8) Instrukcje zarządzania systemem monitoringu wizyjnego.

§ 3

1. Infrastruktura teleinformatyczna zakładu obejmująca budynki zlokalizowane w Krakowie przy ul. Skarbowej 1 i 4, al. Focha 33, ul. Batorego 3 i ul. Kapelanka 60, w których znajdują się pomieszczenia lub ich części w obszarze przetwarzania danych osobowych.
2. Przetwarzanie danych osobowych może wystąpić w większości pomieszczeń zakładu, jednakże ze względu na koncentrację pełnionych funkcji, szczególnie chronione powinny być pomieszczenia serwerowni, pomieszczenia, w których przechowuje się i składowe kopie zapasowe, archiwum, pomieszczenia rejestracji pacjentów, dane pracowników i kontrahentów.
3. Wykaz pomieszczeń lub ich części tworzących w zakładzie obszar, w którym przetwarzane są dane osobowe oraz sposób ich zabezpieczenia zawiera dokumentacja prowadzona przez Pełnomocnika ds. Administrowania Danymi Osobowymi- *Inspektora Ochrony Danych Osobowych*, zgodnie ze wzorem stanowiącym załącznik nr 1 do niniejszej polityki.
4. Pełnomocnik ds. Administrowania Danymi Osobowymi- *Inspektor Ochrony Danych Osobowych* zobowiązany jest do prowadzenia bieżącej aktualizacji wykazu określonego w ust. 3.

§ 4

1. Wykaz zbiorów danych osobowych gromadzonych i przetwarzanych w zakładzie w systemie informatycznym oraz programów zastosowanych do przetwarzania tych

danych w formie elektronicznej zawiera dokumentacja prowadzona przez Pełnomocnika ds. Administrowania Danymi Osobowymi- *Inspektora Ochrony Danych Osobowych*, zgodnie ze wzorem stanowiącym załącznik nr 2 do niniejszej polityki.

2. Pełnomocnik ds. Administrowania Danymi Osobowymi- *Inspektor Ochrony Danych Osobowych* zobowiązany jest do prowadzenia bieżącej aktualizacji wykazu określonego w ust. 1.
3. Administrator Systemu Informatycznego zobowiązany jest informować Pełnomocnika ds. Administrowania Danymi Osobowymi- *Inspektora Ochrony Danych Osobowych* o zmianie programów określonych w ust. 1.

§ 5

Strukturę zbiorów danych osobowych i zawartość poszczególnych pól informacyjnych tworzą:

- 1) dane osobowe przetwarzane w systemie informatycznym w formie elektronicznej i tradycyjnej papierowej,
- 2) dane osobowe przetwarzane w zbiorach danych, zestawach oraz pojedynczych informacjach osobowych,
- 3) dane przetwarzane za pomocą monitoringu wizyjnego

§ 6

1. Rejestr czynności przetwarzania danych osobowych zawiera wszystkie procesy i zabezpieczenia danych osobowych, które są przetwarzane w zakładzie według wymagań zawartych w art. 30 ust 1 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.
2. Rejestr czynności przetwarzania danych osobowych prowadzi Pełnomocnik ds. Administrowania Danymi Osobowymi- *Inspektor Ochrony Danych Osobowych*, który zobowiązany jest do prowadzenia bieżącej aktualizacji rejestru określonego w ust. 1.

§ 7

1. Rejestr kategorii czynności przetwarzania prowadzony jest kiedy przetwarzane dane osobowe są przetwarzane przez jednostki zewnętrzne współpracujące z zakładem zgodnie z wymaganiami zawartymi w art. 30 ust 2 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.
2. Rejestr kategorii czynności przetwarzania prowadzi Pełnomocnik ds. Administrowania Danymi Osobowymi- *Inspektor Ochrony Danych Osobowych*, który zobowiązany jest do prowadzenia bieżącej aktualizacji rejestru określonego w ust. 1.

§ 8

1. Z uwagi na charakter przetwarzania danych osobowych zakład zobowiązany jest do Oceny skutków dla ochrony danych tzw. oceny *analizy ryzyka bezpieczeństwa zasobów Szpitala Specjalistycznego im. J. Dietla w Krakowie w zakresie ochrony danych osobowych*

2. Powyższa ocena skutków dla ochrony danych prowadzona jest wspólnie przez pełnomocnika ds. Administrowania Danymi Osobowymi- Inspektora Ochrony Danych Osobowych oraz Administratora Systemu Informatycznego, która następnie jest przedstawiana Dyrektorowi Zakładu, stanowiąca rekomendację do zmian w systemie zarządzania procesem przetwarzania danych osobowych na terenie zakładu.
3. Każdorazowa zmiana, lub zmiany organizacyjne w funkcjonowaniu systemów przetwarzania danych osobowych wymagają przygotowania aktualizacji oceny skutków dla ochrony danych osobowych.
4. *Metodyka Oceny skutków dla ochrony danych tzw. oceny analizy ryzyka bezpieczeństwa zasobów Szpitala Specjalistycznego im. J. Dietla w Krakowie w zakresie ochrony danych osobowych jest przeprowadzana zgodnie z załącznikiem nr 3 do niniejszej polityki*

§ 9

1. Zakład, ze względu na połączenie z siecią publiczną, zobowiązany jest stosować środki bezpieczeństwa przetwarzania danych osobowych w formie elektronicznej, w systemie informatycznym określony w ustawie o systemie informacji w ochronie zdrowia (Dz. U. 2011 Nr. 113 poz. 657) z późniejszymi zmianami.
2. Zakład analizuje i zapobiega zagrożeniom dla przetwarzanych i gromadzonych danych osobowych, którymi są:
 - 1) połączenie z siecią internet,
 - 2) niebezpieczeństwo pożarów, włamań, kradzieży,
 - 3) błędy ludzkie, które dzielą się na:
 - a) świadome, obejmujące:
 - ujawnianie przez użytkownika elektronicznego systemu informatycznego identyfikatora i hasła dostępu do systemu współpracownikom i osobom obcym,
 - udostępnianie stanowisk pracy wraz z danymi osobowymi osobom nieuprawnionym,
 - udostępnianie osobom nieuprawnionym programów komputerowych zainstalowanych w elektronicznym systemie informatycznym,
 - używanie oprogramowania zainstalowanego w elektronicznym systemie informatycznym, w innym zakresie niż pozwala na to umowa licencyjna,
 - przenoszenie programów komputerowych, dysków twardych z jednego stanowiska na inne,
 - kopiowanie danych na nośniki informacji, kopiowanie na inne systemy celem wyniesienia poza zakład,
 - samowolne instalowanie i używanie jakichkolwiek programów komputerowych, w tym również programów do użytku prywatnego,
 - używanie nośników danych udostępnionych przez osoby postronne,
 - otwieranie załączników i wiadomości poczty elektronicznej od nieznanych nadawców,
 - używanie nośników danych niesprawdzonych, niewiadomego pochodzenia lub niezwiązanych z wykonywaną pracą,
 - tworzenie kopii zapasowych niechronionych hasłem i/lub bez odpowiednich zabezpieczeń miejsca ich przechowywania,
 - narażanie urządzeń komputerowych i nośników danych na kradzież, w tym pozostawienie komputera przenośnego w miejscu publicznym lub w samochodzie bez zabezpieczenia,

- wyrzucanie dokumentów zawierających dane osobowe bez uprzedniego ich trwałego zniszczenia uniemożliwiającego ich odczytanie lub odtworzenie,
 - pozostawianie dokumentów na biurku po zakończonej pracy, pozostawianie otwartych dokumentów na ekranie monitora bez blokady konsoli,
 - ignorowanie nieznanych osób poruszających się w obszarze przetwarzania danych osobowych,
 - ignorowanie przepisów, zasad i wymaganych działań z zakresu danych osobowych,
- b) nieświadome, obejmujące:
- zapominanie o wylogowaniu się z systemu komputerowego przed opuszczeniem pomieszczenia,
 - złe ustawienie monitora komputerowego, które umożliwia wgląd w ekran z wyświetlonymi danymi osobowymi osobom postronnym,
 - pozostawianie bez nadzoru osób trzecich przebywających w pomieszczeniach zakładu, w których przetwarzane są dane osobowe,
 - pozostawianie zewnętrznych nośników informacji podłączonych do obsługiwanego komputera, tj. zewnętrznych dysków, pamięci flash (pendrive), dyskietek i płyt w napędzie,
 - zapisywanie na kartkach i pozostawianie haseł wejściowych w miejscach widocznych dla innych osób,
 - pozostawianie dokumentów, kopii dokumentów zawierających dane osobowe w drukarkach, kserokopiarkach lub w miejscach wydruku,
 - pozostawianie kluczy w drzwiach szaf i biur, zostawianie otwartych pomieszczeń, w których przetwarza się dane osobowe.

§ 10

Zakład stosuje środki techniczne i organizacyjne służące zapewnieniu poufności, integralności i rozliczalności przetwarzania danych w formie elektronicznej w ramach systemu informatycznego i w formie tradycyjnej papierowej.

1. Zasady:

- 1) ochrony danych osobowych przetwarzanych w formie elektronicznej,
- 2) ochrony systemu informatycznego służącego do przetwarzania danych osobowych w formie elektronicznej,
- 3) ochrony oprogramowania systemu informatycznego służącego do przetwarzania danych osobowych w formie elektronicznej,
- 4) tworzenia kopii bezpieczeństwa ich przechowywanie i ochrony, zostały uregulowane w „Instrukcji Zarządzania Systemem Informatycznym” zamieszczonej w rozdziale III niniejszego opracowania.
- 5) Instrukcja zarządzania monitoringiem wizyjnym

2. Ochrona danych osobowych przetwarzanych i zamieszczanych w dokumentach sporządzonych w formie tradycyjnej papierowej odbywa się zgodnie z następującymi zasadami:

- dane osobowe przetwarzane i zamieszczane w dokumentach sporządzanych w formie papierowej gromadzone są w zbiorach, które stanowią rejestry, księgi, zeszyty oraz segregatory,
- zbiory zawierające dane osobowe dokumentów sporządzonych w formie papierowej podlegają przechowywaniu w pomieszczeniach odpowiednio zabezpieczonych,
- obszary przetwarzania i gromadzenia danych osobowych zamieszczanych w dokumentach sporządzanych w formie papierowej zabezpiecza się przed dostępem osób postronnych, a ich przebywanie na tym obszarze może nastąpić za zgodą kierownika komórki, której to dotyczy,

- sposób postępowania z kluczami do pomieszczeń należących do obszaru przetwarzania i gromadzenia danych osobowych zamieszczanych w dokumentach sporządzanych w formie papierowej przy użyciu tradycyjnych środków pisarskich i zabezpieczania tych pomieszczeń został określony w ust. 5.
3. W zakresie nadawania prawa dostępu do systemu informatycznego i przetwarzania danych osobowych obowiązują następujące procedury:
- do przetwarzania danych osobowych i obsługi systemu informatycznego muszą być dopuszczone osoby wykonujące zadania na rzecz zakładu i posiadające prawo dostępu do zasobów informatycznych w postaci upoważnienia nadanego przez Pełnomocnika ds. Administrowania Danymi Osobowymi – *Inspektora Ochrony Danych Osobowych*, które uzyskują status użytkownika systemu informatycznego, wzór upoważnienia określa załącznik nr 4 do niniejszej polityki,
 - prawo dostępu do systemu informatycznego w postaci upoważnienia do przetwarzania danych osobowych sporządzane jest w dwóch egzemplarzach, z których jeden otrzymuje Administrator Systemu Informatycznego, a drugi jest umieszczany w aktach osobowych lub innej dokumentacji osoby upoważnionej do przetwarzania danych osobowych,
 - upoważnienia do przetwarzania danych osobowych i obsługi systemu informatycznego wydawane są na podstawie prowadzonego w zakładzie wykazu stanowisk, na których wymagane jest upoważnienie do przetwarzania danych osobowych, prowadzonego przez Pełnomocnika ds. Administrowania Danymi Osobowymi - *Inspektora Ochrony Danych Osobowych*, wzór wykazu określa załącznik nr 5 do niniejszej polityki,
 - ewidencję osób upoważnionych do przetwarzania danych osobowych i obsługi systemu informatycznego, prowadzi Pełnomocnik ds. Administrowania Danymi Osobowymi – *Inspektor Ochrony Danych Osobowych*, wzór ewidencji zawiera załącznik nr 6 do niniejszej polityki,
 - ewidencja powinna zawierać następujące dane:
 - imię i nazwisko osoby upoważnionej,
 - wskazanie stanowiska pracy i jednostki lub komórki organizacyjnej, w której użytkownik wykonuje zadania na rzecz zakładu,
 - identyfikator nadawany przez Administratora Systemu Informatycznego, po przedstawieniu przez użytkownika prawa dostępu do zasobów informatycznych,
 - użytkownikowi nie wolno udostępniać nadanego mu identyfikatora i hasła innym osobom pod groźbą odpowiedzialności wynikających z przepisów prawa dotyczących ochrony danych osobowych,
4. Ochrona przeciwpożarowa obszaru, w którym przetwarzane są dane osobowe odbywa się w następujący sposób:
- pomieszczenia zakładu, w których pracują urządzenia elektronicznego systemu informatycznego bez nadzoru, a w szczególności pomieszczenia z serwerami pracującymi w systemie pracy ciągłej, powinny być wyposażone w elektroniczny system wykrywania pożaru z czujkami reagującymi na ogień, dym, temperaturę,
 - sygnalizacja alarmu powinna być objęta całodobowym monitoringiem,
 - system alarmowy powinien być objęty stałym nadzorem specjalistycznym, a czujki okresowo sprawdzane,
5. Ochrona fizyczna budynków i pomieszczeń, w których przetwarzane są dane osobowe, odbywa się w następujący sposób:
- Pełnomocnik ds. Administrowania Danymi Osobowymi – *Inspektor Ochrony Danych Osobowych* wydaje zalecenia/rekomendacje w sprawie wdrożenia zabezpieczeń techniczno – organizacyjnych zbiorów danych osobowych, które będą realizowane przez poszczególne komórki organizacyjne zakładu.

- kierownicy jednostek i komórek organizacyjnych zakładu ponoszą odpowiedzialność za realizację wytycznych w zakresie zabezpieczeń fizycznych zbiorów danych osobowych w podległych jednostkach i komórkach,
- budynki i pomieszczenia zakładu lub ich części, w których przetwarzane są dane osobowe, powinny być zabezpieczone w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym, w czasie nieobecności osoby, która posiada upoważnienie do przetwarzania tych danych,
- budynki i pomieszczenia zakładu lub ich części, w których przetwarzane są dane osobowe, muszą posiadać, co najmniej następujące zabezpieczenia:
 - drzwi do pomieszczeń powinny być zamykane na klucz,
 - dokumenty z danymi osobowymi po zakończeniu pracy powinny być chowane w biurkach, szafach lub sejfach zamykanych na klucz, a klucze od nich należy przechowywać w szufladzie zamykanej na zamek,
 - budynek musi podlegać ochronie i/lub monitorowaniu w systemie 24 godzinnym przez pracowników ochrony fizycznej (portierów), zobowiązanych do ochrony osób i mienia na terenie poszczególnych budynków,
- pomieszczenia biurowe tworzące obszary, w których przetwarzane są dane osobowe w poszczególnych budynkach zakładu, są miejscami podlegającymi szczególnej ochronie, a zatem po godzinach pracy drzwi wejściowe do tych pomieszczeń powinny być bezwzględnie zamykane przez ostatnią kończącą pracę osobę, która posiada upoważnienie do przetwarzania tych danych, zobowiązaną do przekazania kluczy od drzwi pracownikowi ochrony fizycznej (portierowi), przy czym przekazanie portierowi kluczy przez poszczególne osoby, które posiadają upoważnienie do przetwarzania tych danych, jest momentem przekazania pomieszczenia pod ochronę,
- klucze do drzwi wejściowych pomieszczeń biurowych tworzących obszary, w których przetwarzane są dane osobowe w poszczególnych budynkach zakładu, przechowywane są na portierniach w zamykanych gablotach, a wydawanie kluczy przez portierów następuje tylko do rąk osób upoważnionych ujętych w wykazie upoważnionych do pobierania kluczy i po odnotowaniu wydania w książce ewidencji wydanych kluczy **czytelny podpisem**,

6. Szkolenia z zakresu danych osobowych:

- każdy użytkownik powinien mieć świadomość zagrożeń wpływających na bezpieczeństwo przetwarzania danych osobowych w zakładzie,
- każda nowa osoba, której powierzono wykonywanie zadań na rzecz zakładu powinna być zapoznana z ogólnymi zasadami i przepisami dotyczącymi bezpieczeństwa przetwarzania danych osobowych w zakładzie, a szczególnie wynikających z norm prawa o ochronie danych osobowych i niniejszej polityki,
- w miarę potrzeby należy przeprowadzać szkolenia z udziałem osób, którym powierzono wykonywanie zadań na rzecz zakładu, omawiając problematykę bezpieczeństwa danych osobowych w zakładzie, ze szczególnym uwzględnieniem nowych uregulowań prawnych, które powinny zorientować te osoby w skali zagrożeń oraz uświadomić rangę zabezpieczeń, zwłaszcza stosowanych na poziomie użytkownika oraz informować o grożących konsekwencjach w sytuacjach lekceważenia zasad bezpieczeństwa przy przetwarzaniu danych osobowych w zakładzie,
- formę i tematykę szkoleń z zakresu ochrony danych osobowych w zakładzie, ich rodzaj oraz częstotliwość określa Pełnomocnik ds. Administrowania Danymi Osobowymi – *Inspektor Ochrony Danych Osobowych* w porozumieniu z Dyrektorem zakładu i Administratorem Systemów Informatycznych.

7. Karty dostępu

1. Osoby pracujące w budynkach szpitala oraz upoważnione przez Dyрекcję Szpitala zostają wyposażone w elektroniczne karty dostępowe.

2. Karty dostępne służą do uzyskania wejścia do chronionych pomieszczeń oraz uruchamiania niektórych usług w tych pomieszczeniach (zasilanie, oświetlenie),
 3. Aby uzyskać kartę należy minimum dwa dni robocze wcześniej zgłosić zapotrzebowanie do Sekcji Informatyki. Pracownik Sekcji Informatyki na podstawie miejsca pracy danego pracownika przygotowuje odpowiednią kartę.
 4. Wydanie imiennej karty i hasła jest ewidencjonowane. Od tego momentu każde użycie karty lub hasła zostaje zaewidencjonowane w systemie kontroli dostępu.
 5. Pracownik Sekcji Informatyki jest zobowiązany do przeszkolenia pracownika w zakresie obsługi systemu.
 6. Po rozwiązaniu umowy o pracę lub ustaniu innych relacji prawnych wobec zakładu z użytkownikiem należy bezzwłocznie kartę dostępową zwrócić do Sekcji Informatyki.
 7. Jeśli Pracownik zagubi kartę należy bezzwłocznie powiadomić Sekcję Informatyki o zaistniałym fakcie. Uprawnienia przypisane karcie zostaną natychmiast zablokowane.
 8. W przypadku nieposiadania karty przy sobie należy posługiwać się hasłem – uprawnienia hasła, są identyczne z uprawnieniami karty.
 9. W przypadku nieposiadania karty i niepamiętania hasła należy pobrać z portierni kartę tymczasową (pobranie odbywa się za pisemnym i imiennym potwierdzeniem wydania takiej karty). Po zakończeniu pracy w danym dniu kartę należy zwrócić.
 10. Zabrania się użyczania kart osobom trzecim.
8. Instrukcja Zarządzania systemem monitoringu
1. Instrukcja zarządzania monitoringiem wizyjnym stanowi załącznik nr 7 do niniejszej polityki.

§ 11

1. Naruszenie przepisów o ochronie danych osobowych jest zagrożone sankcjami karnymi wynikającymi z Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (art. 107 i 108) oraz Kodeksu Karnego (art. 130, 266 – 269, 287), jak i również sankcjami finansowymi oraz odpowiedzialnością cywilną.
2. Niezależnie od odpowiedzialności przewidzianej w przepisach wskazanych w ust. 1, naruszenie zasad ochrony danych osobowych obowiązujących w zakładzie może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością porządkową oraz rozwiązaniem umowy o pracę za wypowiedzeniem lub bez wypowiedzenia z winy pracownika, względnie rozwiązaniem umowy zawartej z osobą, której powierzono wykonywanie zadań na rzecz zakładu na podstawie innego tytułu niż umowa o pracę .

§ 12

1. Udostępnianie danych osobowych poza zakład może odbywać się za zgodą Administratora Danych lub osoby przez niego upoważnionej na podstawie obowiązujących przepisów norm prawa i zarządzeń wewnętrznymi Dyrektora Zakładu.
2. Dane osobowe mogą zostać udostępnione na pisemny umotywowany wniosek podmiotu korporacyjnego lub osoby fizycznej zainteresowanej ich uzyskaniem.
3. Rejestr wniosków udostępnienia danych osobowych i odmów zawierających dane osobowe prowadzi Sekretariat Szpitala lub odpowiednie komórki organizacyjne, które udostępniają dokumentację zgodnie zobowiązującymi normami prawa i zarządzeń wewnętrznych Dyrektora zakładu, które podlegają kontroli przez Pełnomocnika ds. Administrowania Danymi Osobowymi – Inspektora Ochrony Danych Osobowych.

4. Dane osobowe, w szczególnych przypadkach, mogą być udostępniane w trybie innym niż wnioskowy, którego rejestr prowadzony jest przez Sekretariat Szpitala.
Do przypadków szczególnych należy zaliczyć sytuacje zagrożenia życia i zdrowia pacjenta oraz udzielenia informacji w przypadkach społecznie uzasadnionych.
5. Dane osobowe zawarte w dokumentacjach medycznych udostępnia się zgodnie z zarządzeniem Dyrektora zakładu w sprawie wprowadzenia instrukcji udostępniania dokumentacji medycznej.
6. Udostępnianie danych osobowych kontrahentom zakładu może następować wyłącznie w realizacji zawartych z nimi umów lub porozumień, w których powinny być zamieszczone klauzule zobowiązujące ich do skutecznej należytej ochrony udostępnionych im danych osobowych oraz przetwarzania ich wyłącznie do celów określonych w umowie lub porozumieniu i w sposób zgodny z obowiązującymi przepisami prawa.
7. Udostępnianie danych do celów określonych w ust. 6 następuje w sposób gwarantujący bezpieczeństwo tych danych.

§ 13

1. Przez naruszenie ochrony danych osobowych w zakładzie rozumie się:
 - 1) stwierdzone naruszenie zabezpieczenia elektronicznego systemu informatycznego,
 - 2) sytuacje, w których stan urządzeń, zawartość zbioru danych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczenia danych,
 - 3) stwierdzone naruszenie zabezpieczenia dokumentacji w formie papierowej, zaginięcie dokumentu, próba jego powielenia, samowolnego wyniesienia poza teren zakładu względnie udostępnienia w sposób niezgodny z postanowieniem § 12,
 - 4) udostępnienie danych osobom nieupoważnionym, zabieranie nośników zawierających dane osobowe przez osoby nieuprawnione, przetwarzanie danych z naruszeniem norm prawa z zakresu ochrony danych osobowych oraz ich zmianę, utratę, uszkodzenie lub zniszczenie
 - 5) naruszenie dostępu do pomieszczeń, w których są przechowywane lub przetwarzane dane osobowe.
2. Każda osoba, której powierzono wykonywanie zadań na rzecz zakładu, a w szczególności osoba, która posiada upoważnienie do przetwarzania danych osobowych jest obowiązana niezwłocznie powiadomić o zaistniałym przypadku naruszenia ochrony danych osobowych w zakładzie Pełnomocnika ds. Administrowania Danymi Osobowymi - Inspektora Ochrony Danych Osobowych.
3. O przypadku naruszenia ochrony danych osobowych w zakładzie Pełnomocnik ds. Administrowania Danymi Osobowymi - Inspektor Ochrony Danych Osobowych jest obowiązany:
 - 1) niezwłocznie zawiadomić Dyrektora zakładu,
 - 2) zarejestrować fakt naruszenia danych osobowych poprzez sporządzenie notatki z podaniem miejsca, daty i przypuszczalnego zakresu ich naruszenia,
 - 3) podjąć natychmiastowe działania zmierzające do usunięcia stwierdzonych naruszeń,
 - 4) ustalić osobę odpowiedzialną za zaistniałą sytuację,
 - 5) przeprowadzić analizę aktualnego sposobu zabezpieczenia danych,
 - 6) przedstawić propozycję naprawy systemu, która uniemożliwi w przyszłości naruszenie danych osobowych na obszarze ich przetwarzania
 - 7) wyłączyć z użytku pomieszczenie, w którym doszło do naruszenia ochrony danych osobowych, do momentu usunięcia przyczyn tego naruszenia,
 - 8) w przypadku naruszenia danych w systemie informatycznym wspólnie z Administratorem Systemu Informatycznego ustala zakres naruszenia danych elektronicznych z równoczesnym blokowaniem ścieżki naruszenia ochrony (sieć, końcówka, konto użytkownika) do momentu ustalenia przyczyn naruszenia i ich usunięcia.

4. Pełnomocnik ds. Administrowania Danymi Osobowymi - Inspektor Ochrony Danych Osobowych przygotowuje pisemny wniosek do osoby lub podmiotu korporacyjnego o zwrot danych osobowych, w których posiadanie weszły niezgodnie z prawem, który przedstawia Dyrektorowi zakładu. W przypadku danych elektronicznych wniosek przygotowuje w porozumieniu z Administratorem Systemu Informatycznego.

§ 14

1. Zgłoszenie naruszenia danych osobowych do organów nadzorczych dochodzi wtedy, gdy doszło do naruszenia praw i wolności osób fizycznych, zgodnie z art.33 RODO
2. Każdy pracownik Szpitala Specjalistycznego im. J. Dietla w Krakowie oraz inna osoba zobowiązana do przestrzegania Polityki Bezpieczeństwa Informacji, która była świadkiem lub otrzymała informację o naruszeniu danych osobowych w podmiocie niezwłocznie jest zobowiązana do powiadomienia Administratora Danych Osobowych o zdarzeniu, podać wszelkie istotne informacje mogące pomóc w ustaleniu przyczyny naruszenia zasad ochrony danych osobowych.
3. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Pełnomocnikowi ds. Administrowania Danymi Osobowymi - Inspektorowi Ochrony Danych Osobowych.
4. W przypadku stwierdzenia wystąpienia incydentu naruszenia ochrony danych osobowych, administrator powinien zgłosić je organowi nadzorcemu bez zbędnej zwłoki – jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – chyba że administrator jest w stanie wykazać zgodnie z zasadą rozliczalności, że jest mało prawdopodobne, by to naruszenie danych osobowych mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych. Jeżeli nie można wnieść zgłoszenia w terminie 72 godzin, powinno mu towarzyszyć wyjaśnienie przyczyn opóźnienia, a informacje mogą być przekazywane stopniowo, bez dalszej zbędnej zwłoki.
5. Pełnomocnik ds. Administrowania Danymi Osobowymi - Inspektor Ochrony Danych Osobowych zobowiązany jest do prowadzenia rejestru incydentów zgodnie z wzorem stanowiącym załącznik nr 8 do niniejszej instrukcji.

§ 15

Zarządzanie przetwarzaniem danych osobowych w zakładzie należy do:

- 1) Pełnomocnika ds. Administrowania Danymi Osobowymi- *Inspektora Ochrony Danych Osobowych*,
- 2) Administratora Systemów Informatycznych.

§ 16

1. Pełnomocnik ds. Administrowania Danymi Osobowymi- *Inspektor Ochrony Danych Osobowych* odpowiedzialny jest za nadzorowanie i koordynowanie w zakładzie zasad postępowania przy przetwarzaniu danych osobowych.
2. Do podstawowych zadań Pełnomocnika ds. Administrowania Danymi Osobowymi- *Inspektora Ochrony Danych Osobowych* należy w szczególności:
 - 1) tworzenie wewnętrznej dokumentacji zgodnie z obowiązującymi przepisami prawa w zakresie przetwarzania i gromadzenia danych osobowych,
 - 2) współpraca z jednostkami i komórkami organizacyjnymi zakładu, w których przetwarzane i gromadzone są dane osobowe i udzielanie im w tym zakresie wskazówek i porad, kontrolowanie przestrzegania zasad bezpieczeństwa przetwarzania danych,
 - 3) nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników systemu informatycznego,

- 4) prowadzenie wykazu stanowisk w zakładzie, na których wymagane jest upoważnienie do przetwarzania danych osobowych,
- 5) udzielanie upoważnień do przetwarzania danych osobowych i obsługi systemu informatycznego,
- 6) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych i obsługi systemu informatycznego,
- 7) opracowywanie wytycznych mających zastosowanie przy wdrażaniu i doskonaleniu niniejszej polityki oraz nadzór nad jej przestrzeganiem,
- 8) prowadzi rejestr czynności przetwarzania danych osobowych,
- 9) prowadzi rejestr kategorii czynności przetwarzania,
- 10) nadzór nad fizycznym zabezpieczeniem pomieszczeń zakładu, w których przetwarzane są dane osobowe,
- 11) nadzór i kontrola nad przestrzeganiem w zakładzie obowiązków wynikających z przepisów norm prawa z zakresu danych osobowych,
- 12) zapewnienie dostępu do przetwarzania danych osobowych wyłącznie przez osoby upoważnione mogące wykonywać wyłącznie uprawnione operacje,
- 13) szkolenia osób dopuszczonych do przetwarzania danych osobowych, w tym ich zaznajamianie i szkolenie z przepisami prawa z zakresu ochrony danych osobowych i postanowieniami zawartymi w niniejszej polityce oraz odbieranie od nich oświadczeń o odbyciu takiego szkolenia
- 14) prowadzenie rejestru osób dopuszczonych do przetwarzania danych osobowych,
- 15) nadzór nad przekazywaniem danych osobowych na zewnątrz zakładu,
- 16) opracowywanie dla Dyrektora zakładu rocznego planu poprawy bezpieczeństwa przetwarzania danych (propozycje zakupowe, organizacyjne, szkoleniowe).
- 17) Tworzy Ocenę skutków dla ochrony danych tzw. Analiza ryzyka przetwarzania danych osobowych, która jest wspólnie z Administratorem Systemu Informatycznego - ponieważ ryzyko utraty danych wiąże się zarówno po stronie informatycznej oraz tradycyjnej, ocena ryzyka ma wpływ na podejmowanie decyzji, które mogą wpłynąć na funkcjonowanie zakładu.

§ 17

1. Administrator Systemu Informatycznego odpowiedzialny jest za administrowanie systemem informatycznym przetwarzającym dane osobowe zgodnie z zasadami niniejszej polityki.
2. Administrowanie systemem informatycznym w zakładzie odbywa się według Instrukcji Zarządzania Systemem Informatycznym.
3. Administrator Systemu Informatycznego w porozumieniu z Pełnomocnikiem ds. Administrowania Danymi Osobowymi- *Inspektorem Ochrony Danych Osobowych* może powołać Lokalnego Administratora Systemu Informatycznego.

§ 18

1. Lokalny Administrator Systemu Informatycznego odpowiedzialny jest za administrowanie wyznaczonym systemem informatycznym przetwarzającym dane osobowe.

§ 19

1. Realizacja niniejszej polityki powinna być poddawana przeglądowi przez Pełnomocnika ds. Administrowania Danymi Osobowymi- *Inspektora Ochrony Danych Osobowych* nie rzadziej niż raz w roku.

2. Pełnomocnik ds. Administrowania Danymi Osobowymi-Administrator Bezpieczeństwa Informacji po dokonaniu przeglądu określonego w ust. 1 sporządza raport roczny, w którym przedstawia stan realizacji niniejszej polityki. Raport podlega przedstawieniu Dyrektorowi zakładu najpóźniej do dnia 15 lutego następnego roku.
3. Treść polityki jest aktualizowana w przypadku wprowadzenia lub zmiany środków technicznych lub organizacyjnych służących ochronie danych osobowych zawartych w systemach elektronicznych oraz zamieszczonych w dokumentach sporządzanych w formie papierowej przy użyciu tradycyjnych środków pisarskich.

ROZDZIAŁ III

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

§ 20

Instrukcja zarządzania systemami informatycznymi jest dokumentem eksploatacyjnym, regulującym zasady oraz procedury zarządzania i administrowania systemem informatycznym zakładu. Instrukcja obejmuje swoim zakresem wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w systemach informatycznych, w szczególności zaś osoby pełniące funkcje:

- 1) Pełnomocnika ds. Administrowania Danymi Osobowymi – Inspektor Ochrony Danych Osobowych,
- 2) Administratora Systemu Informatycznego (ASI),
- 3) Lokalnego Administratora Systemu Informatycznego (LASI),
- 4) kierowników jednostek i komórek organizacyjnych.

§ 21

1. W skład systemu informatycznego zakładu wchodzi:
 - 1) sieć LAN/WA,
 - 2) serwery,
 - 3) stanowiska komputerowe (obejmujące komputery, terminale oraz inne urządzenia będące wyposażeniem stanowiska pracy),
 - 4) oprogramowanie systemowe,
 - 5) aplikacje i programy użytkowe,
 - 6) urządzenia i oprogramowanie zabezpieczające przed nieupoważnionym dostępem,
 - 7) urządzenia awaryjnego zasilania,
 - 8) urządzenia kopii zapasowych,
 - 9) system kont pocztowych,
 - 10) strona WWW,
2. Poziom bezpieczeństwa systemu informatycznego w zakładzie określony zgodnie z ustawą o systemie informacji w ochronie zdrowia (Dz. U. 2011 Nr. 113 poz. 657) z późniejszymi zmianami.
3. Sieć LAN/WAN – sieć znajdująca się w budynkach przy ul Skarbowej 1 i 4, al. Focha 33 oraz przy ul Batorego 3.
 - 1) Sieć LAN jest połączona z siecią WAN w jednym punkcie poprzez router brzegowy oraz urządzenie typu firewall wraz z odpowiednim oprogramowaniem.
 - 2) Sieć LAN/WAN jest używana do realizacji celów statutowych zakładu.

- 3) W przypadku konieczności połączenia lokalnych sieci LAN administrowanych poprzez zakład poprzez sieć WAN używa się urządzeń/oprogramowania wykorzystujących protokół VPN.
- 4) Następujące czynności:
- a) podłączania stanowisk komputerowych do internetu poprzez modemy lub inne urządzenia,
 - b) podłączania do sieci LAN sprzętu komputerowego, którego właścicielem nie jest zakład,
 - c) udostępniania sieci osobom innym niż użytkownicy systemu informacyjnego,
 - d) używania oprogramowania służącego do penetracji sieci,
 - e) dokonywania modyfikacji sieci LAN,
- mogą być wykonane wyłącznie za zgodą Administratora Systemu Informacyjnego.
4. Serwery, w tym serwery aplikacji, serwery pamięci masowych oraz serwery aplikacji/danych podlegają szczególnej ochronie polegającej na:
- 1) kontroli dostępu do pomieszczeń serwerowni,
 - 2) zabezpieczeniu w urządzeniu zasilania awaryjnego,
 - 3) wyposażeniu serwerów w zwielokrotnione zasilanie,
 - 4) utrzymywaniu odpowiedniej temperatury pracy,
 - 5) okresowemu przeglądowi technicznemu,
 - 6) zabezpieczeniu aplikacji i danych oprogramowaniem antywirusowym,
 - 7) zabezpieczeniu przed niepowołanym dostępem do serwerów.
5. Stanowiska komputerowe stanowiące wyposażenie stanowiska pracy, w tym:
- 1) komputery,
 - 2) terminale,
 - 3) aparatura medyczna i diagnostyczna,
- podlegają ochronie przed dostępem osób nieupoważnionych, jakimkolwiek modyfikacjom sprzętowym lub modyfikacjom istniejącego na nich oprogramowania, korzystania w sposób sprzeczny z niniejszą instrukcją oraz polityką.
6. Oprogramowanie systemowe zainstalowane na serwerach podlega szczególnej ochronie polegającej na:
- 1) instalacji oprogramowania antywirusowego,
 - 2) pełnej kontroli dostępu użytkowników do systemu,
 - 3) wykonywania kopii bezpieczeństwa systemu,
 - 4) instalacji aktualizacji w systemach,
 - 5) okresowemu przeglądowi systemu.
7. Oprogramowanie systemowe zainstalowane na stanowiskach komputerowych podlega ochronie polegającej na:
- 1) instalacji oprogramowania antywirusowego (o ile to jest możliwe),
 - 2) instalacji aktualizacji,
 - 3) rocznemu przeglądowi systemu.
- Jednocześnie zabrania się użytkownikom ingerowania w system, samodzielnego instalowania bądź usuwania elementów składowych systemu.
8. Aplikacje i programy użytkowe dzielą się ze względu na dane w nich przetwarzane na:
- 1) ogólnoużytkowe,
 - 2) przetwarzające dane osobowe – podlegające szczególnej ochronie oraz kontroli polegającej na:
 - a) używaniu systemu uwierzytelniania użytkownika zgodnie z wymogami rozporządzenia,
 - b) wykonywaniu kopii zapasowych danych i aplikacji,
 - c) nadzorze nad prawidłową pracą aplikacji.

9. Jeżeli jest to wymagane urządzenia i oprogramowanie zabezpieczające przed nieupoważnionym dostępem ochraniają sieć LAN zakładu, jak również poszczególne serwery oraz stanowiska komputerowe. Obecnie Sieć LAN jest chroniona przez urządzenie typu „*firewall - zaporą ogniową*” spełniające minimalne wymagania stawiane takim systemom – dostosowane do ilości użytkowników, rodzaju danych przetwarzanych w systemie. Serwery oraz newralgiczne stanowiska komputerowe wyposażone są w oprogramowanie typu „*firewall - zaporą ogniową*”. Na tych samych urządzeniach należy również zadbać w szczególny sposób o instalację wszelkich aktualizacji dot. zabezpieczeń systemu.
10. W urządzenia awaryjnego zasilania wyposażone są wszystkie serwery i inne urządzenia mające istotny wpływ na pracę systemu. Jakość i moc tych urządzeń jest tak dobrana aby zapewnić bezpieczne wyłączenie systemu, a dla krótkotrwałej przerwy w dostawie prądu <30 min. ciągłą pracę. Serwery oraz pamięci masowe zasilane są zawsze poprzez min 2 niezależne zasilacze podłączone do 2 różnych urządzeń UPS.
11. Urządzenia kopii zapasowych wykorzystywane są do regularnego wykonywania kopii, zarówno systemu operacyjnego, jak również danych i aplikacji. Nośnikiem danych kopii są nośniki optyczne, magnetyczne oraz elektroniczne. System tworzenia kopii zapasowych zawarty jest w § 25 .
12. System kont pocztowych, jak i strona WWW znajdują się na serwerze zewnętrznym. Administratorem kont pocztowych, jak również strony WWW jest Sekcja Informatyki. Zabrania się umieszczania na stronie WWW jakichkolwiek danych osobowych. Dane osobowe mogą być przekazywane przy użyciu kont pocztowych tylko w sposób zaszyfrowany.
13. Dane osobowe przetwarzane są w systemie informatycznym w celu realizacji zadań wynikających ze statutu zakładu oraz innych przepisów odnoszących się do jego działalności.
14. Zabrania się kopiowania i przenoszenia danych osobowych na nośnikach nie należących do Szpitala – nośniki prywatne, telefony prywatne itp.

§ 22

1. Administratorem Systemu Informatycznego w zakładzie jest Kierownik Sekcji Informatyki, a w przypadku jego nieobecności osoba przez niego wyznaczona.
2. Do podstawowych zadań Administratora Systemu Informatycznego należy w szczególności:
 - 1) zapewnianie awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych w zakładzie,
 - 2) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe,
 - 3) zarządzanie identyfikatorami i hasłami użytkowników, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji,
 - 4) nadzór nad czynnościami związanymi ze sprawdzaniem systemu informatycznego pod kątem obecności wirusów komputerowych, częstotliwości ich sprawdzania oraz nadzorowanie uaktualniania systemów antywirusowych i ich konfiguracji,
 - 5) nadzór nad wykonywaniem kopii zabezpieczających, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych,
 - 6) nadzór nad przeglądami, konserwacjami oraz uaktualnianiem obsługiwanego systemu informatycznego w zakładzie oraz wszelkimi czynnościami administracyjnymi wykonywanymi na bazach danych osobowych,

- 7) nadzór nad prawidłową pracą sieci komputerowej;
- 8) tworzenie, jeżeli istnieją odpowiednie możliwości, warunków technicznych umożliwiających automatyczne wyłączanie się ekranów monitorów, na których przetwarzane są dane osobowe, po upływie ustalonego czasu nieaktywności użytkownika,
- 9) podejmowanie natychmiastowych działań zabezpieczających stan obsługiwanego systemu informatycznego, w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu lub informacji o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych osobowych,
- 10) bieżący monitoring oraz zapewnianie ciągłości działania obsługiwanego systemu informatycznego,
- 11) optymalizacja wydajności obsługiwanego systemu informatycznego,
- 12) instalacje i konfiguracje sprzętu sieciowego i serwerowego,
- 13) instalacje i konfiguracje oprogramowania systemowego i sieciowego,
- 14) konfiguracja i administracja oprogramowaniem systemowym i sieciowym zabezpieczającym dane osobowe przed nieupoważnionym dostępem,
- 15) współpraca z dostawcami usług i sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych,
- 16) weryfikacja możliwości integracji systemów informatycznych służących przetwarzaniu danych osobowych w formie elektronicznej,
- 17) opracowywanie procedur określających zarządzanie obsługiwanym systemem informatycznym,
- 18) prowadzenie zakupów urządzeń komputerowych i peryferyjnych, sieciowych i serwerowych,
- 19) wnioskowanie o rekomendacje do Pełnomocnika ds. Administrowania Danymi Osobowymi - Inspektora Ochrony Danych Osobowych w sprawie procedur bezpieczeństwa i standardów zabezpieczeń,
- 20) współpraca z dostawcami aplikacji,
- 21) zapewnianie przeszkolenia użytkowników w zakresie prawidłowego korzystania z aplikacji bazodanowych zgodnie z powierzonymi im obowiązkami,
- 22) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
- 23) zarządzanie, sprawowanie nadzoru oraz serwis urządzeń komputerowych pracujących w obsługiwanym systemie informatycznym,
- 24) diagnozowaniu zdarzeń i usuwaniu awarii urządzeń komputerowych w zakładzie,
- 25) konfiguracja i administracja oprogramowaniem systemowym na stacjach roboczych zabezpieczającym dane osobowe przed nieupoważnionym dostępem,
- 26) prowadzenie ewidencji sprzętu i oprogramowania wykorzystywanego w obsługiwanym systemie informatycznym,
- 27) instalacja nowo kupionych urządzeń komputerowych na podstawie zapotrzebowań otrzymanych z poszczególnych jednostek i komórek organizacyjnych zakładu,
- 28) realizacja umów z podmiotami świadczącymi usługi serwisu urządzeń komputerowych,
- 29) koordynacja działań zapewniających sprawne funkcjonowanie i zabezpieczenie obsługiwanego systemu informatycznego przed niepowołanym dostępem,
- 30) analiza raportów wszelkich zdarzeń związanych z bezpieczeństwem systemów przetwarzania informacji chronionych, otrzymywanych od Lokalnych Administratorów Systemów Informatycznych,
- 31) dopuszczanie systemów przetwarzania informacji do eksploatacji,
- 32) zapewnienie zgodność wszystkich wdrażanych systemów przetwarzania danych osobowych chronionych z niniejszą polityką
- 33) zatwierdzanie procedur bezpieczeństwa i standardów zabezpieczeń obsługiwanego systemu informatycznego zawnioskowanych przez Lokalnych Administratorów Systemów Informatycznych,

- 34) weryfikacja i zatwierdzenie projektów rozwoju obsługiwanego systemu informatycznego, służącego do przetwarzania danych osobowych w formie elektronicznej,
- 35) określanie standardów dotyczących urządzeń komputerowych, sieci komputerowej, oprogramowania systemowego oraz aplikacji pracujących w obsługiwanym systemie informatycznym w oparciu o informacje od Lokalnych Administratorów Systemów Informatycznych,
- 36) opracowywanie dla Dyrektora zakładu rocznego planu poprawy bezpieczeństwa przetwarzania danych w systemie informatycznym (propozycje zakupowe, organizacyjne, szkoleniowe),
- 37) prowadzenie rejestru podmiotów korporacyjnych, którym są przekazywane dane osobowe w formie elektronicznej, zawierającego:
 - a) nazwę podmiotu,
 - b) wskazanie podstawy prawnej lub umowy,
 - c) określenie formy przekazywanych danych (nośnik),
 - d) wskazanie osoby odpowiedzialnej za przekazywanie danych.
- 38) Prowadzenie ewidencji użytkowników systemu informatycznego, która powinna zawierać następujące dane:
 - a) imię i nazwisko osoby upoważnionej,
 - b) wskazanie stanowiska pracy i jednostki lub komórki organizacyjnej, w której użytkownik jest zatrudniony,
 - c) identyfikator nadawany przez Administratora Systemu Informatycznego, po przedstawieniu przez użytkownika prawa dostępu do zasobów informatycznych.
- 39) tworzy Ocenę skutków dla ochrony danych tzw. Analiza ryzyka przetwarzania danych osobowych, która jest wspólnie tworzona z Pełnomocnikiem ds. Ochrony Danych Osobowych - Inspektorem Ochrony Danych Osobowych - ponieważ ryzyko utraty danych wiąże się zarówno po stronie informatycznej oraz tradycyjnej, ocena ryzyka ma wpływ na podejmowanie decyzje, które mogą wpłynąć na funkcjonowanie zakładu.

§ 23

- 1. Lokalnym Administratorem Sytemu Informatycznego jest osoba wyznaczona przez Kierownika komórki, w której używane jest oprogramowanie służące do przetwarzania danych. Lokalny Administrator Sytemu Informatycznego wyznaczany jest w porozumieniu z Administratorem Systemu Informatycznego oraz za zgodą Pełnomocnika ds. Administrowania Danymi Osobowymi – Inspektora Ochrony Danymi Osobowymi.
- 2. Lokalny Administrator Sytemu Informatycznego wykonuje obowiązki administratora wydzielonego oprogramowania, a w szczególności:
 - 1) zapewnienie należytej ochrony danych osobowych przetwarzanych i gromadzonych w wydzielonym oprogramowaniu,
 - 2) zapewnienie przetwarzania danych osobowych zgodnie z obowiązującym prawem,
 - 3) przechowywanie danych osobowych w postaci umożliwiających identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania,
 - 4) wyznaczanie użytkowników systemu informatycznego upoważnionych do przetwarzania danych osobowych w wydzielonym oprogramowaniu,
 - 5) dokonywanie zmian użytkowników systemu informatycznego upoważnionych do przetwarzania danych osobowych w wydzielonym oprogramowaniu,
 - 6) przestrzeganie przyjętych dla systemu informatycznego zasad bezpieczeństwa,
 - 7) reagowanie na naruszanie bezpieczeństwa systemu informatycznego i usuwanie jego skutków w wydzielonym oprogramowaniu,

- 8) nadzorowanie właściwego użytkowania wydzielonego oprogramowania;
- 9) zapewnienie wykonywania kopii bezpieczeństwa informatycznych baz danych oraz systemów informatycznych w wydzielonym oprogramowaniu - w porozumieniu z Sekcją Informatyki,
- 10) zapewnienie poprawności merytorycznej przetwarzania danych osobowych gromadzonych w lokalnych zbiorach danych,
- 11) określanie miejsca i czasu przetwarzania, przechowywania, tworzenia i niszczenia nośników zawierających dane osobowe,

§ 24

1. Użytkownikiem systemu informatycznego może zostać tylko osoba posiadająca ważne upoważnienie do przetwarzania danych osobowych wydane przez Pełnomocnika ds. Administrowania Danymi osobowymi- *Inspektora Ochrony Danych Osobowych*.
2. Na podstawie przedłożonego przez użytkownika upoważnienia określonego w ust. 1 pracownicy Sekcji Informatyki zakładu zakładają konto o następujących parametrach:
 - 1) identyfikator użytkownika: nazwisko użytkownika, a przypadku istnienia już konta o takim samym identyfikatorze – nazwisko wraz z ustalonym z użytkownikiem ciągiem znaków,
 - 2) okresem ważności konta w systemie wygasa z dniem ustania stosunku pracy,
 - 3) zakresem przetwarzanych danych: zależy od grupy zawodowej oraz pełnionych obowiązków,
 - 4) dostępem do zasobów: zależy od grupy zawodowej oraz pełnionych obowiązków.
3. Modyfikacja parametrów konta użytkownika, może nastąpić wskutek:
 - 1) wniosku Pełnomocnika ds. Administrowania Danymi Osobowymi - Inspektora Ochrony Danych Osobowych ,
 - 2) wniosku Działu Kadr zakładu,
 - 3) wniosku kierownika jednostki lub komórki organizacyjnej zakładu, w której dany użytkownik rozpoczyna lub kończy przetwarzanie danych,
 - 4) wniosku przełożonego użytkownika,
 - 5) ustania stosunku pracy lub obowiązywania umowy,
 - 6) zmianą miejsca wykonywania zadań przez osobę upoważnioną.
4. Kasowanie konta. Operacja nie występuje w systemie informatycznym. Dezaktywacja konta następuje poprzez modyfikację daty ważności konta. Identyfikator użytkownika jest przechowywany w systemie jako dana o użytkowniku wprowadzającym/modyfikującym dane.
5. Każdy nowy użytkownik systemu informatycznego przed uzyskaniem dostępu do systemu informatycznego musi przejść podstawowe szkolenie z zakresu obsługi systemu. Szkolenie prowadzi Administrator Systemu Informatycznego lub osoba przez niego wyznaczona. Harmonogram szkoleń dostępny jest w Sekcji Informatyki.
6. Do podstawowych obowiązków każdego użytkownika systemu informatycznego należy:
 - 1) przestrzeganie zapisów niniejszej instrukcji i polityki,
 - 2) zmiana hasła dostępu do systemu następuje co 30 dni,
 - 3) zabezpieczenie danych dostępowych do systemu przed ich nieupoważnionym wykorzystaniem,
 - 4) zabezpieczenie stanowiska wykonywania zadań przed nieupoważnionym dostępem poprzez blokadę dostępu lub wyłączeniem stanowiska komputerowego,
 - 5) wyłączenie stanowiska komputerowego podczas zakańczania pracy,

- 6) zabezpieczenie pomieszczenia, w którym przetwarzane są dane osobowe przed dostępem nieupoważnionych osób,
 - 7) zgłaszanie naruszeń dostępu do systemu informatycznego w sposób określony w § 13 ust.2,
 - 8) prowadzenie ewidencji udostępnień danych osobowych w formie elektronicznej.
- 9) Przy pracy poza systemem HIS/PACS użytkownik wykonuje kopie zapasowe danych na wydzielonych zasobach sieciowych udostępnionych przez Sekcję Informatyki. –
7. Zabrania się użytkownikom:
- 1) dokonywania samodzielnej modyfikacji sprzętu, oprogramowania systemowego oraz aplikacyjnego,
 - 2) modyfikacji parametrów oprogramowania antywirusowego,
 - 3) udostępniania stacji roboczych do konserwacji lub naprawy bez porozumienia z Administratorem Systemu Informatycznego,
 - 4) przyłączania do gniazd sieci komputerowych zakładu urządzeń bez zgody pracowników Sekcji Informatyki zakładu,
 - 5) zmiany lokalizacji urządzeń połączonych do sieci komputerowej zakładu bez zgody pracowników Sekcji Informatyki zakładu
 - 8) używania oprogramowania w innym zakresie niż pozwala na to umowa licencyjna,
 - 9) kopiowania danych na nośniki informacji, kopiowania na inne systemy celem wynoszenia ich poza zakład,
 - 10) używania nośników danych udostępnionych przez osoby postronne,
 - 11) otwierania załączników i wiadomości poczty elektronicznej od nieznanych i nie zaufanych nadawców..

§ 25

1. Zbiory danych w systemie informatycznym są zabezpieczane przed utratą lub uszkodzeniem za pomocą:
 - 1) urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej,
 - 2) sporządzania kopii zapasowych zbiorów danych (kopie pełne i kopie przyrostowe).
2. Za tworzenie kopii bezpieczeństwa systemu informatycznego odpowiedzialny jest Administrator Systemu Informatycznego lub wyznaczona przez niego osoba.
3. Pełne kopie zapasowe zbiorów danych (na nośnikach zewnętrznych) są tworzone dwa razy na tydzień,
4. Robocze kopie zapasowe zbiorów danych wykonywane są codziennie.
5. W szczególnych przypadkach – przed aktualizacją lub zmianą w systemie należy bezwarunkowo wykonać pełną kopię zapasową systemu.
6. Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu. Za przeprowadzanie tej procedury odpowiedzialny jest Administrator Systemu Informatycznego.
7. Okresowe kopie zapasowe wykonywane są na elektronicznych nośnikach informacji. Kopie powinny być przechowywane w innych pomieszczeniach niż te, w których przechowywane są zbiory danych osobowych wykorzystywane na bieżąco, muszą być zabezpieczone przed zniszczeniem oraz temperaturą. Kopie zapasowe przechowuje się w sposób uniemożliwiający nieuprawnione przejęcie, modyfikację, uszkodzenie lub zniszczenie.
8. Dostęp do nośników z kopiami zapasowymi systemu oraz kopiami danych osobowych, ma wyłącznie Pełnomocnik ds. Administrowania Danymi Osobowymi - Inspektor

Ochrony Danych Osobowych oraz Administrator Systemu Informatycznego, którego kopie zawierają konkretne nośniki.

9. W przypadku kopii zapasowych sporządzanych indywidualnie przez użytkownika odpowiedzialnością za ich zniszczenie obarczony jest użytkownik.
10. W przypadku nośników informacji, przez ich zniszczenie rozumie się ich trwałe i nieodwracalne zniszczenie fizyczne do stanu nie dającego możliwości ich rekonstrukcji i odzyskania danych.
11. W przypadku braku możliwości zrealizowania procedury zniszczenia nośników informacji przez użytkownika, należy fakt ten zgłosić Administratorowi Systemu Informatycznego, który po przekazaniu mu nośników zapewni ich zniszczenie w ramach środków technicznych Sekcji Informatyki bądź poddanie procedurze utylizacji nośników informacji realizowanej przez firmę zewnętrzną.

PRZEPISY KOŃCOWE

§ 26

1. Upoważnienia do przetwarzania danych osobowych wydane przed 25 maja 2018 r. zachowują ważność do momentu ich wycofania, a także rozwiązania lub wygaśnięcia stosunku pracy.
2. Z uwagi na zmianę podstawy prawnej upoważnienia zmienia się w upoważnieniu ta część, a zakres, cel i okres ważności upoważnienia pozostaje bez zmian.