Załącznik nr 1_do Zarządzenia nr 41/2015_Rektora
Warszawskiego Uniwersytetu Medycznego z dnia 28 maja 2015 r.

POLITYKA BEZPIECZEŃSTWA

Rozdział I Postanowienia ogólne.

Rozdział II Deklaracja intencji, cele i zakres polityki bezpieczeństwa.

Rozdział III Obowiązki i odpowiedzialność w zakresie zarządzania bezpieczeństwem.

Rozdział IV Obszary przetwarzania danych.

Rozdział V Struktury zbiorów danych oraz przepływ danych pomiędzy systemami.

Rozdział VI Środki ochrony.

Rozdział VII Postępowanie w sytuacjach naruszenia zasad ochrony danych osobowych.

Rozdział VII Postanowienia końcowe.

Załącznik nr 1 Tabela form naruszeń zasad ochrony danych osobowych

Załącznik nr 2 Raport o naruszeniu zasad ochrony danych osobowych (wzór)

Rektor Warszawskiego Uniwersytetu Medycznego (WUM), jako Administrator Danych Osobowych Uczelni wprowadzając Politykę Bezpieczeństwa Informacji deklaruje pełne zaangażowanie dla zapewnienia bezpieczeństwa przetwarzanych informacji, w tym danych osobowych oraz wsparcie dla przedsięwzięć technicznych i organizacyjnych związanych z ochroną informacji.

Kierownictwo Uniwersytetu zobowiązuje się do podejmowania niezbędnych działań mających na celu zapewnienie ochrony informacji na pożądanym poziomie, a tym samym spełnienie wymaganego poziomu bezpieczeństwa systemów informacyjnych.

Niniejsza Polityka uwzględnia w swojej treści wymogi rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie krajowych ram interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2012 r. poz. 526) oraz regulacjami wynikającymi z rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (Dz. U. z 2002 r. Nr 100 poz. 1024) w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Rozdział I
Postanowienia ogólne.

§ 1

Ilekroć w Polityce mowa jest o:

1) systemie informatycznym należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
2) zabezpieczeniu danych w systemie należy przez to rozumieć wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
3) wewnętrznej sieci teleinformatycznej, należy przez to rozumieć sieć Administratora, łączącą co najmniej dwa indywidualne stanowiska komputerowe, umożliwiającą użytkownikom określony dostęp do danych.

Rozdział II
Deklaracja intencji, cele i zakres polityki bezpieczeństwa.

§ 2

1. Warszawski Uniwersytet Medyczny, jako podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.
2. Celem Polityki jest ochrona danych osobowych, przetwarzanych w jednostkach organizacyjnych WUM i ochrona przed udostępnieniem ich osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed zmianą, uszkodzeniem lub zniszczeniem.

§ 3

1. Polityka Bezpieczeństwa porządkuje kwestie związane z bezpieczeństwem informacji i przetwarzania danych osobowych w Warszawskim Uniwersytecie Medycznym i zawiera najważniejsze zasady postępowania obejmujące:
   1) zapewnienie spełnienia wymagań prawnych;

2) ochronę systemów przetwarzania informacji przed nieuprawnionym dostępem bądź zniszczeniem;
3) podnoszenie świadomości pracowników;
4) zmniejszenie ryzyka utraty informacji;
5) zaangażowanie wszystkich pracowników w ochronę informacji.

2. Zakresem Polityki bezpieczeństwa objęte są :
   1) wszystkie istniejące, obecnie lub w przyszłości systemy informacyjne oraz tradycyjne (papierowe), w których przetwarzane są lub będą informacje;
   2) informacje będące własnością Uniwersytetu, lub klientów o ile zostały przekazane na podstawie umów;
   3) wszystkie typy nośników informacji na których są lub będą znajdować się informacje;
   4) wszystkie lokalizacje (pomieszczenia), w których są lub będą przetwarzane informacje;
   5) wszyscy pracownicy w rozumieniu Kodeksu Pracy, studenci i inne osoby majce dostęp do informacji na zasadach określonych w Polityce Bezpieczeństwa;
   6) informacje mogą być przetwarzane wyłącznie w systemach, które spełniają warunki opisane w polityce bezpieczeństwa.

§ 4

1. Polityka określa podstawowe zasady bezpieczeństwa i zarządzania bezpieczeństwem systemów oraz zbiorów, w których są przetwarzane dane osobowe.
2. Polityka dotyczy wszystkich danych osobowych, przetwarzanych w jednostkach organizacyjnych Warszawskiego Uniwersytetu Medycznego (WUM), niezależnie od formy ich przetwarzania (zbiory ewidencyjne, systemy informatyczne) oraz od tego czy dane są lub mogą być przetwarzane w zbiorach danych.
3. Polityka ma zastosowanie wobec wszystkich jednostek organizacyjnych Uczelni.
4. Obowiązkiem pracowników jest bezwzględne przestrzeganie postanowień niniejszej Polityki Bezpieczeństwa informacji WUM.

§ 5

1. Cele Polityki realizowane są poprzez zapewnienie danym osobowym następujących cech:
   1) **poufności - właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom;**
   2) **integralności - właściwości zapewniającej, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;**
   3) **rozliczalności - właściwości zapewniającej, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.**
2. Za podmiot nieupoważniony uważa się podmiot, który nie otrzymał zgody Administratora na udostępnienie mu danych osobowych w celu włączenia ich do zbioru oraz osobę nieposiadającą upoważnienia do przetwarzania danych osobowych, nadanego przez Administratora.

§ 6

Dla skutecznej realizacji Polityki Administrator zapewnia:
1) odpowiednie do zagrożeń i kategorii danych objętych ochroną, środki techniczne i rozwiązania organizacyjne;
2) szkolenia w zakresie przetwarzania danych osobowych i sposobów ich ochrony;
3) okresowe szacowanie ryzyka zagrożeń dla zbiorów danych;
4) kontrolę i nadzór nad przetwarzaniem danych osobowych;
5) monitorowanie zastosowanych środków ochrony.

Rozdział III
Obowiązki i odpowiedzialność w zakresie zarządzania bezpieczeństwem.

§ 7

1. Zarządzanie bezpieczeństwem systemów jest procesem ciągłym, realizowanym przy współdziałaniu użytkowników z Administratorem Bezpieczeństwa Informacji (ABI) i Administratorem Systemu Informatycznego (ASI).
2. W celu skutecznej realizacji Polityki Administrator może powołać Lokalnych Administratorów przetwarzania danych (LADO) działających w mniejszych obszarach struktur organizacyjnych lub obszarach wyszczególnionych przedmiotowo np. rekrutacja, projekty itp.
3. Wszystkie osoby przetwarzające dane osobowe po otrzymaniu odpowiedniego upoważnienia (wzór formularza 4.6) od Administratora lub właściwego LADO i złożeniu oświadczenia (wzór formularza 4.5) zobowiązane są do:
   1) przetwarzania danych osobowych zgodnie z obowiązującymi przepisami;
   2) postępowania zgodnie z ustaloną przez Administratora Polityką, Instrukcją i Regulaminem, o których mowa w Zarządzeniu.
4. W przypadku naruszenia przepisów lub zasad postępowania użytkownik podlega odpowiedzialności służbowej i karnej.

§ 8

1. Do zadań Administratora Bezpieczeństwa Informacji (ABI) należy:
   1) koordynowanie przedsięwzięć określonych zakresem Polityki w § 3 ust.2;
   2) występowanie do Administratora o cofnięcie, ograniczenie lub odmowę wyrażenia zgody na przyznanie uprawnień do przetwarzania danych osobowych;
   3) przygotowywanie projektów zarządzeń, instrukcji i wytycznych Administratora;
   4) organizowanie bądź prowadzenie szkoleń w zakresie ochrony danych osobowych dla pracowników uczelni;
   5) prowadzenie dokumentacji odzwierciedlającej wykonywanie zadań z zakresu ochrony danych osobowych i baz danych, zgodnie z formularzami przedkładanymi ze strony LADO i kierowników komórek organizacyjnych:
      a) ewidencji miejsc, w których przetwarzane są dane osobowe w Uczelni – formularz 4.1 „Wykaz budynków i pomieszczeń, w których są przetwarzane dane osobowe w Warszawskim Uniwersytecie Medycznym",
      b) ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych i ich identyfikatorów w systemach informatycznych – Formularz 4.2 „Ewidencja osób upoważnionych do przetwarzania danych osobowych w tradycyjnych zbiorach danych i w systemach informatycznych Warszawskiego Uniwersytetu Medycznego",
      c) ewidencji zbiorów danych osobowych w WUM i sposobu ich zabezpieczania. Formularz 4.3 „Wykaz zbiorów danych tradycyjnych i w systemach informatycznych, w których są przetwarzane dane osobowe w Warszawskim Uniwersytecie Medycznym";
   6) wnioskowanie do LADO i kierowników jednostek o uzupełnienie danych, zawartych w ww. formularzach;
   7) zgłaszanie i aktualizowanie ewentualnych zbiorów wrażliwych danych osobowych do rejestracji w GIODO;
   8) prowadzenie planowych rocznych sprawdzeń[1] i przedstawianie ADO sprawozdania

[1] Sprawdzenie – należy przez to rozumieć czynności mające na celu zweryfikowanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych w szczególności w wyniku zwrócenia się o dokonanie sprawdzenia przez Generalnego Inspektora Ochrony Danych Osobowych.

z tych sprawdzeń wg zasad określonych w przepisach zewnętrznych;
9) prowadzenie sprawdzeń na zlecenie GIODO i przesłanie do zlecającego sprawozdania z przeprowadzonego sprawdzenia;
10) nadzór nad weryfikacją i aktualizacją „Polityki bezpieczeństwa" oraz Instrukcji zarządzania systemem informatycznym";
11) przekazywanie Administratorowi wniosku o przekazywaniu danych osobowych do państwa trzeciego;
12) prowadzenie na podstawie upoważnienia korespondencji z GIODO w imieniu Administratora;
13) okresowe przekazywanie Administratorowi informacji dotyczących naruszeń bezpieczeństwa ochrony danych;
14) ścisła współpraca z ASI i kierownikiem Działu Informatyki w celu zapewnienia ochrony danych;
15) prowadzenie wewnętrznego rejestru zbiorów danych osobowych przetwarzanych w Uczelni w formie papierowej.

2. Do zadań i obowiązków LADO przy zachowaniu ścisłej współpracy z ABI, należy:
1) określanie indywidualnych obowiązków i odpowiedzialności osób zatrudnionych przy przetwarzaniu danych osobowych, wynikających z ustawy o ochronie danych osobowych, w postaci upoważnień (Formularz 4.7);
2) zapewnienie warunków osobom do zapoznania się z obowiązującymi, w tym zakresie przepisami zatrudnionym przy przetwarzaniu danych osobowych;
3) przekazywanie pracownikom zaleceń ABI w zakresie ochrony danych osobowych i baz danych funkcjonujących w podległych im jednostkach systemach tradycyjnych i informatycznych oraz nadzór nad wykonaniem;
4) nadzór nad przekazywaniem na bieżąco do ABI, aktualnych danych z komórek organizacyjnych;
5) stwarzanie warunków organizacyjnych i technicznych umożliwiających spełnienie wymogów wynikających z obowiązywania ustawy o ochronie danych osobowych w podległych im jednostkach.

3. Zobowiązuje się wszystkich LADO oraz Kierownika Biura Organizacyjnego do okresowego przekazywania do ABI w terminach do **15 lipca każdego roku**, wg stanu na dzień 30 czerwca oraz do **15 stycznia każdego roku** wg stanu na dzień 31 grudnia ubiegłego roku informacji obejmujących:
1) ewidencje baz danych, w których przetwarzane są dane osobowe metodą tradycyjną lub poprzez systemy informatyczne;
2) wykazu osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych i ich identyfikatorów systemowych;
3) wykazu miejsc przetwarzania danych osobowych w systemach informatycznych w podległych im jednostkach;
4) ocen i wniosków wynikających z zagrożeń bezpieczeństwa i analizy stanu ochrony obszarów przetwarzania danych osobowych;

4. Zobowiązuje się ABI do koordynowania zadań określonych w ust. 3 oraz do zgromadzenia i aktualizowania wszystkich wymaganych dokumentów.

5. Dane aktualizacyjne należy przekazywać do ABI na właściwych formularzach 4.1, 4.2, 4.3 (określonych w załączniku nr 4 do Zarządzenia) w formie elektronicznej.

6. W terminie **14 dni** od wydania upoważnienia LADO oraz Kierownik Biura Organizacyjnego są zobowiązani do przekazania do Działu Personalnego kopii wydanych upoważnień oraz oświadczeń pracowników o zapoznaniu się z aktualnymi przepisami dotyczącymi ochrony danych osobowych w Uczelni oraz zachowaniu w tajemnicy zasad ochrony danych osobowych.

7. Dział Personalny zobowiązany jest do bieżącego uzupełniania akt osobowych pracowników

Uczelni zatrudnionych przy przetwarzaniu danych osobowych o:

1) kopie imiennych upoważnień do dostępu do zbiorów danych tradycyjnych bądź systemu informatycznego, w którym przetwarzane są dane osobowe, wydane przez Administratora;
2) oświadczenie pracownika o zapoznaniu się z aktualnymi przepisami dotyczącymi ochrony danych osobowych w Uczelni oraz zachowaniu w tajemnicy zasad ochrony danych osobowych.

8. Do zadań i obowiązków ASI należy nadawanie, ograniczanie lub cofanie identyfikatorów i nadawanie, ograniczanie lub cofanie uprawnień użytkownikom, opisane w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, w § 3 ust. 2 i 3, oraz w § 4 ust. 1 (stanowiącym załącznik nr 3 do Zarządzenia) wraz z uaktualnianiem kont i uprawnień użytkowników systemu w porozumieniu z ABI oraz:
   1) zakładanie, modyfikacja lub usuwanie baz danych;
   2) migracja danych pomiędzy bazami;
   3) zabezpieczanie danych w sposób uniemożliwiający ich identyfikację w bazach danych na podstawie pisemnego polecenia osób, o których mowa w § 1 ust. 1 Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
   4) archiwizowanie danych ze zbiorów;
   5) wykonywanie kopii zapasowych baz danych osobowych;
   6) zarządzanie bazą antywirusową, w tym określanie warunków działania oprogramowania przy zachowaniu maksymalnej efektywności i minimalizacji jej negatywnego wpływu na korzystanie przez użytkowników z systemu;
   7) realizację przedsięwzięć mających na celu wdrażanie technicznych i logicznych zabezpieczeń chroniących system przed nieuprawnionym dostępem do danych oraz reagowanie w przypadku naruszenia bądź powstania zagrożenia bezpieczeństwa danych przetwarzanych w systemie;
   8) instalowanie, aktualizowanie i konfigurowanie oprogramowania systemowego i aplikacyjnego oraz urządzeń, o ile czynności te nie są wykonywane przez upoważnionych przedstawicieli dostawcy systemu na podstawie zawartej umowy;
   9) przygotowywanie urządzeń, dysków i innych elektronicznych nośników informacji, zawierających dane osobowe, do likwidacji, przekazania innemu podmiotowi, konserwacji lub naprawy;
   10) przekazywania do ABI opisów struktur zbiorów danych, schematów przepływu danych pomiędzy systemami, zawartości poszczególnych pól informacyjnych w aplikacjach oraz wszelkich zmian w tym zakresie;
   11) natychmiastowe informowanie ABI o zdarzeniach, o których mowa w pkt. 7;
   12) wykonywanie bieżącej konserwacji i przeglądu systemu.

§ 9

1. Użytkownicy przeprowadzają codzienną kontrolę bezpieczeństwa systemu przetwarzania danych osobowych na stanowiskach pracy.
2. Zasady postępowania w sytuacji wystąpienia lub podejrzenia wystąpienia naruszenia bezpieczeństwa określone zostały w Rozdziale VII „Postępowanie w sytuacjach naruszenia zasad ochrony danych osobowych".

Rozdział IV
Obszary przetwarzania danych.

§ 10

Za obszar przetwarzania danych uznaje się miejsce wykonywania jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.

§ 11

1. Kierownicy jednostek organizacyjnych Uczelni zobowiązani są do przekazywania do ABI informacji o zmianach w lokalizacji miejsc przetwarzania danych osobowych, wydanych (unieważnionych) upoważnieniach oraz w wykazach przetwarzanych zbiorów w terminie do 14 dni od dokonania zmian.
2. Dane aktualizacyjne należy przekazywać do ABI na właściwych formularzach (określonych w załączniku nr 4 do Zarządzenia) w formie elektronicznej.
3. LADO przekazują do ABI (w terminach określonych i w formie ustalonej przez ABI) oceny i wnioski wynikające z zagrożeń bezpieczeństwa i analizy stanu ochrony obszarów przetwarzania danych osobowych we właściwych dla LADO jednostkach organizacyjnych.

§ 12

Kierownicy jednostek organizacyjnych Uczelni osób przedkładają do właściwych administratorów danych osobowych (Rektora WUM lub właściwego LADO) wnioski o nadanie, cofnięcie lub zmianę upoważnień do przetwarzania danych osobowych dla pracowników i innych .

§ 13

Kierownicy jednostek organizacyjnych Uczelni zobowiązani są do niezwłocznego przekazywania do ABI wykazu zbiorów oraz programów zastosowanych do przetwarzania danych osobowych, o których mowa w § 8 ust.1 pkt.5, lit. a-c.

Rozdział V
Struktury zbiorów danych oraz przepływ danych pomiędzy systemami.

§ 14

1. Dane osobowe są przetwarzane przy zastosowaniu systemów informatycznych, w zbiorach ewidencyjnych oraz poza zbiorami.
2. Zbiory danych osobowych zlokalizowane są w przedmiotowych bazach danych umieszczonych na serwerach bazodanowych.
3. Dane osobowe w zbiorach są przetwarzane tylko w aplikacjach (programach) dostosowanych do merytorycznych potrzeb jednostek organizacyjnych WUM.

§ 15

1. Zawartość pól informacyjnych, występujących w aplikacjach (programach) systemów zastosowanych do przetwarzania danych, musi być zgodna z przepisami prawa, które uprawniają lub zobowiązują Administratora do przetwarzania danych osobowych.
2. Na żądanie Administratora, osoby, o których mowa w § 11 ust. 1, zobowiązane są wskazać podstawy prawne określające zakres przetwarzanych danych.

§ 16

1. Opisy struktur zbiorów danych wskazujące zawartość poszczególnych pól informacyjnych i powiązania pomiędzy nimi, wykonują ASI na podstawie aplikacji zastosowanych do przetwarzania tych danych.
2. Opisy wykonywane są w postaci wydruków zrzutów ekranowych lub struktur tablic bazy prezentujących zawartość pól informacyjnych i powiązań pomiędzy nimi.
   W przypadku braku możliwości uzyskania wydruku zrzutu ekranowego ASI sporządzają inne dostępne opisy struktury zbioru.
3. ASI zobowiązani są do przekazywania opisów do ABI oraz natychmiastowego informowania ABI o wszelkich w nich zmianach.

§ 17

1. Schematy przepływu danych pomiędzy systemami informatycznymi, zastosowanymi w celu przetwarzania danych osobowych wykonują ASI, zgodnie z relacjami występującymi w programach służących do przetwarzania danych osobowych.
2. ASI zobowiązani są do przekazywania schematów do ABI oraz natychmiastowego informowania ABI o wszelkich w nich zmianach.

§ 18

1. Przepływ danych pomiędzy systemami zastosowanymi w celu przetwarzania danych osobowych może odbywać się w postaci przepływu jednokierunkowego lub przepływu dwukierunkowego.
2. Przesyłanie danych pomiędzy systemami może odbywać się w sposób manualny, przy wykorzystaniu nośników zewnętrznych (np. dyskietka, CD, DVD, taśma streamera, dysk wymienny, PenDrive itp.) lub w sposób półautomatyczny, przy wykorzystaniu funkcji eksportu (importu) danych za pomocą teletransmisji (np. poprzez wewnętrzną sieć teleinformatyczną).
3. Przesyłanie danych osobowych e-mailem jest dopuszczalne tylko po spełnieniu poniższych wymagań:
   1) w obrębie komputerowej sieci wewnętrznej WUM, gdy nadawca i adresat mają ważne upoważnienie do przetwarzania danych osobowych, oraz do przesyłania danych wykorzystywane są ich służbowe konta pocztowe w domenie WUM.edu.pl – bez konieczności stosowania dodatkowych zabezpieczeń kryptograficznych;
   2) poza komputerową sieć wewnętrzną WUM, gdy nadawca ma ważne upoważnienie do przetwarzania danych osobowych oraz do wysyłki wykorzystuje się służbowe konta pocztowe w domenie wum.edu.pl, a adresatem jest podmiot, z którym WUM ma ważną umowę o przetwarzaniu danych osobowych – w tym przypadku obowiązkowo nadawca musi zastosować techniki kryptograficzne do zabezpieczania danych osobowych.

Rozdział VI
Środki ochrony.

§ 19

1. Administrator zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia **poufności, integralności i rozliczalności przetwarzanych danych**.
2. **Kierownicy jednostek organizacyjnych Warszawskiego Uniwersytetu Medycznego przeprowadzają okresową analizę** ryzyka dla poszczególnych systemów i na tej podstawie przedstawiają Administratorowi lub właściwemu LADO **propozycje dotyczące zastosowania** środków technicznych i organizacyjnych (środków ochrony), celem zapewnienia właściwej ochrony przetwarzanych danych.

3. Analiza ryzyka obejmuje:
   1) identyfikację występujących zagrożeń dla systemów, zbiorów i baz danych;
   2) ocenę dotychczas stosowanej ochrony obszarów przetwarzania danych osobowych;
   3) określenie wielkości ryzyka, tj. prawdopodobieństwa, że określone zagrożenie wykorzysta podatność (słabość) zasobu;
   4) identyfikację obszarów wymagających szczególnych zabezpieczeń.
4. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych osobowych.

§ 20

1. Środki ochrony, zastosowane przez Administratora lub LADO dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych, obejmują:
   1) środki fizyczne;
   2) środki osobowe;
   3) środki techniczne.
2. Środki ochrony fizycznej obejmują:
   1) lokalizację miejsc przetwarzania danych osobowych w pomieszczeniach o ograniczonym i kontrolowanym dostępie;
   2) ustalenie zasad gospodarki kluczami do pomieszczeń i szaf;
   3) wyposażenie pomieszczeń, w których przetwarzane są dane osobowe, we wzmocnione drzwi, odpowiednio zabezpieczone okna, meble, zamknięcia i niezbędne zabezpieczenia alarmowe;
   4) składowanie danych wrażliwych oraz nośników wymiennych i nośników kopii zapasowych, w odpowiednio zabezpieczonych szafach;
   5) odpowiednie wyposażenie i zabezpieczenie pomieszczeń serwerowni.
3. Środki ochrony osobowej obejmują:
   1) dopuszczenie do przetwarzania danych osobowych wyłącznie osób posiadających upoważnienie nadane przez Administratora lub LADO lub osobę upoważnioną przez niego;
   2) zapoznanie tych osób z zasadami przetwarzania danych osobowych oraz obsługą systemu służącego do ich przetwarzania;
   3) odebranie stosownych zobowiązań i oświadczeń; tj. zobowiązania do zachowania w tajemnicy danych i sposobów ich zabezpieczenia oraz oświadczenia o zapoznaniu się z treścią przepisów określających zasady postępowania przy przetwarzaniu danych osobowych, a także z dokumentacją przetwarzania i ochrony danych osobowych.
4. Środki ochrony technicznej obejmują:
   1) mechanizmy kontroli dostępu do systemów i zasobów;
   2) zastosowanie odpowiednich i regularnie aktualizowanych narzędzi ochronnych (programy antywirusowe, ściany ogniowe, itp.);
   3) regularne tworzenie kopii zapasowych zbiorów danych przetwarzanych w systemach informatycznych;
   4) zastosowanie ochrony zasilania.

§ 21

1. Uwzględniając kategorie przetwarzanych danych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka dla poszczególnych systemów, stosuje się następujące poziomy bezpieczeństwa:
   1) podstawowy;
   2) podwyższony;
   3) wysoki.

2. Określenia poziomu bezpieczeństwa systemu informatycznego dokonuje ABI na wniosek kierowników jednostek organizacyjnych.
3. Poziomy bezpieczeństwa odnotowuje się w dokumentacji prowadzonej przez ABI.

§ 22

Systemy informatyczne, którym przypisano poziomy bezpieczeństwa wymienione w § 21 muszą spełniać wymagania wymienione w załączniku do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. 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. Nr 100, poz. 1024 z póź. zm.).

Rozdział VII
Postępowanie w sytuacjach naruszenia zasad ochrony danych osobowych.

§ 23

Polityka Bezpieczeństwa określa procedury postępowania w przypadkach, gdy:
1) stwierdzono naruszenie zasad zabezpieczenia w obszarze przetwarzania danych osobowych - zarówno w systemie informatycznym, jak i w zbiorach nieinformatycznych;
2) stan urządzeń, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci komputerowej mogą wskazywać na naruszenie bezpieczeństwa danych osobowych.

§ 24

1. Za naruszenie zabezpieczenia systemu bądź urządzenia, w którym są przetwarzane dane osobowe, przyjmuje się każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną lub uszkodzenia jakiegokolwiek elementu, a w szczególności:
   1) nieautoryzowany dostęp do danych;
   2) nieautoryzowane modyfikacje lub zniszczenie danych;
   3) udostępnienie danych nieautoryzowanym lub nieuprawnionym podmiotom;
   4) nielegalne ujawnienie danych;
   5) pozyskiwanie danych z nielegalnych źródeł.
2. Tabela form naruszeń zasad ochrony danych osobowych stanowi załącznik nr 1 do Polityki Bezpieczeństwa.

§ 25

1. W przypadku stwierdzenia lub podejrzenia naruszenia zabezpieczenia systemu lub zaistnienia zdarzeń, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik, doktorant, student przetwarzający dane osobowe w Uczelni jest zobowiązany przerwać przetwarzanie tych danych i niezwłocznie powiadomić o zaistniałym zdarzeniu LADO oraz ABI, a następnie powinien postępować stosownie do ich decyzji.
2. Zgłoszenie naruszenia procedur ochrony danych osobowych powinno zawierać:
   1) opis symptomów naruszenia procedur ochrony danych osobowych;
   2) określenie sytuacji i czasu zajścia zdarzenia;
   3) identyfikację rodzaju zaistniałego zdarzenia, w tym określenie skali zniszczeń, metody dostępu do danych osoby nieupoważnionej, itp.;
   4) przedstawienie wszelkich istotnych informacji i dokumentów (wydruków, raportów, innych), mogących wskazywać na przyczynę naruszenia;

5) określenie znanych danej osobie możliwości zabezpieczenia systemu oraz wszelkich działań podjętych po ujawnieniu zdarzenia w celu uniemożliwienia lub ograniczenia dostępu osób nieuprawnionych, minimalizacji szkód i zabezpieczenia śladów naruszenia ochrony danych.

§ 26

ABI w porozumieniu z Administratorem lub LADO podejmuje wszelkie działania mające na celu:

1) minimalizację negatywnych skutków zdarzenia;
2) wyjaśnienie przyczyn i okoliczności zdarzenia;
3) zabezpieczenie dowodów zdarzenia;
4) zapewnienie możliwości dalszego bezpiecznego przetwarzania danych.

§ 27

W celu realizacji działań ABI, za zgodą LADO, ma prawo do podejmowania wszelkich czynności dopuszczonych przez prawo, a w szczególności:

1) żądania wyjaśnień od pracowników;
2) korzystania z pomocy konsultantów;
3) wnioskowania o wydanie zakazu wykonywania pracy w zakresie przetwarzania danych osobowych do czasu przywrócenia możliwości przestrzegania procedur bezpieczeństwa.

§ 28

Odmowa udzielenia wyjaśnień lub współpracy z ABI w obszarze ochrony danych osobowych traktowana będzie, jako naruszenie obowiązków pracowniczych.

§ 29

1. ABI po opanowaniu sytuacji kryzysowej przeprowadza każdorazowo szczegółową analizę i opracowuje w terminie 14 dni od daty zaistnienia zdarzenia raport, (wzór raportu stanowi załącznik nr 2 do Polityki Bezpieczeństwa), w którym przedstawia Administratorowi lub LADO przyczyny i skutki zdarzenia oraz wnioski ograniczające możliwości wystąpienia podobnych zdarzeń w przyszłości wraz z propozycją konkretnych działań.
2. Na podstawie sporządzonych raportów oraz innych działań ABI opracowuje roczny raport sprawozdawczy, który przedstawia Administratorowi w terminie do **31 stycznia** następnego roku.

Rozdział VIII
Postanowienia końcowe

§ 30

Nieprzestrzeganie zasad postępowania określonych w niniejszej Polityce stanowi naruszenie obowiązków pracowniczych i może być podstawą odpowiedzialności dyscyplinarnej określonej w Kodeksie Pracy.

§ 31

Jeżeli skutkiem działania określonego w § 24 jest ujawnienie danych osobowych nieuprawnionej osobie lub podmiotowi, sprawca może zostać pociągnięty do odpowiedzialności karnej wynikającej z przepisów Kodeksu Karnego.