Zarządzenie Nr 68/2012/2013
Rektora Uniwersytetu Kazimierza Wielkiego
z dnia 29 kwietnia 2013 r.

w sprawie wprowadzenia instrukcji regulujących zagadnienia ochrony danych osobowych oraz pracy w systemach informatycznych służących do przetwarzania danych osobowych w Uniwersytecie Kazimierza Wielkiego

Na podstawie Ustawy z dnia 29 sierpnia 1997 r. o Ochronie Danych Osobowych (Dz.U. z 2002 Nr 101, poz. 926 z późn. zm.) oraz 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. z 2004, Nr 100, poz. 1024)

zarządzam,

co następuje:

§ 1

Wprowadzić do użytku służbowego:

1) „Politykę bezpieczeństwa przetwarzania danych osobowych w Uniwersytecie Kazimierza Wielkiego", której treść stanowi załącznik nr 1 do niniejszego zarządzenia.
2) „Instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Uniwersytecie Kazimierza Wielkiego", której treść stanowi załącznik nr 2 do niniejszego zarządzenia.

§ 2

Instrukcje, o których mowa w § 1 pkt 1 i 2 mają zastosowanie na wszystkich stanowiskach pracy, na których przetwarzane są dane osobowe w Uniwersytecie Kazimierza Wielkiego.

§ 3

Z treścią instrukcji, o których mowa w § 1 kierownicy jednostek organizacyjnych zapoznają wszystkich pracowników zatrudnionych w danej jednostce przy przetwarzaniu danych osobowych lub pracujących w systemach informatycznych.

§ 4

W związku z wprowadzeniem niniejszego Zarządzenia uchyla się Pismo okólne Nr 18/2006/2007 Rektora UKW z dnia 15 marca 2007 r. w sprawie określenia zasad postępowania w przypadku zapytań o dane osobowe studentów lub absolwentów UKW.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania z mocą obowiązującą od 1 maja 2013 r.

Rektor

prof. dr hab. Janusz Ostoja-Zagórski

Załącznik Nr 1
do Zarządzenia Nr 68/2012/2013
Rektora UKW z dnia 29.04.2013 r.

POLITYKA BEZPIECZEŃSTWA
przetwarzania danych osobowych
w Uniwersytecie Kazimierza Wielkiego

I. Postanowienia ogólne

§ 1

1. Polityka bezpieczeństwa przetwarzania danych osobowych w Uniwersytecie Kazimierza Wielkiego w Bydgoszczy, zwana dalej „Polityką", jest dokumentem określającym zasady postępowania, stosowane środki techniczne i organizacyjne mające na celu zapewnienie bezpieczeństwa w zakresie ochrony danych osobowych przetwarzanych w zbiorach tradycyjnych (w szczególności w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych) oraz w systemach informatycznych.
2. Uniwersytet Kazimierza Wielkiego w Bydgoszczy, zwany dalej „Uniwersytetem", realizując Politykę dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby te dane były:
   1) przetwarzane zgodnie z prawem,
   2) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane przetwarzaniu niezgodnemu z tymi celami,
   3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
   4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż to jest niezbędne do osiągnięcia celu przetwarzania.
3. Uniwersytet realizując Politykę dąży do systematycznego unowocześniania stosowanych w jego strukturze informatycznych, technicznych i organizacyjnych środków ochrony tych danych w celu zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów o ochronie danych osobowych, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.
4. Polityka została opracowana zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późń. zm.),

zwaną dalej „Ustawą o ochronie danych osobowych” oraz rozporządzeniem 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. z 2004 r. Nr 100, poz. 1024), zwane dalej „Rozporządzeniem MSWiA”.

5. Szczegółowe zasady ochrony danych osobowych przetwarzanych w zbiorach informatycznych Uniwersytetu określa Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.
6. Uzupełnieniem Polityki są:
   1) wykaz zbiorów danych osobowych przetwarzanych w Uniwersytecie wraz z opisem struktury zbiorów danych, wskazującym zawartość poszczególnych pól informacyjnych, ze wskazaniem programów zastosowanych do przetwarzania tych danych i opisem przepływu danych pomiędzy wykorzystywanymi systemami informatycznymi,
   2) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.
7. Oba wykazy prowadzone są i aktualizowane zgodnie z następującymi zmianami w stanie faktycznym przez Administratora Bezpieczeństwa Informacji w ramach nałożonych na niego obowiązków.
8. Niniejszy dokument przeznaczony jest dla pracowników Uniwersytetu zatrudnionych przy przetwarzaniu danych osobowych w Uniwersytecie, dla pozostałych pracowników Uniwersytetu oraz dla pracowników podmiotów zewnętrznych współpracujących z Uniwersytetem przy przetwarzaniu danych osobowych (zwanych dalej „pracownikami podmiotu zewnętrznego”) i stanowić ma praktyczną wykładnię stosownych przepisów.

§ 2

1. Wyjaśnienia używanych pojęć:
   1. dane osobowe – **wszelkie** informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (nazwisko, imię, numer PESEL, data urodzenia, adres, numer konta bankowego, wysokość wynagrodzenia, oceny w nauce, wysokość stypendium, zaległości w opłatach za czesne, numer telefonu itd.),
   2. administrator bezpieczeństwa informacji – osoba wyznaczona przez Rektora odpowiednim zarządzeniem, nadzorującą przestrzeganie zasad ochrony danych osobowych w Uniwersytecie,
   3. administrator systemu informatycznego – osoba nadzorująca funkcjonowanie systemu komputerowego, zwykle w sieci lokalnej; w szczególnych przypadkach administratorem systemu informatycznego może być osoba odpowiedzialna za funkcjonowanie aplikacji przetwarzających dane osobowe na pojedynczym komputerze (np. obsługującym komunikację z bankiem),
   4. zbiór danych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie; w przypadku

Uniwersytetu takimi zbiorami są zbiory studentów, kandydatów na studia, pracowników, czytelników biblioteki itp.,

5. przetwarzanie danych osobowych – **jakiekolwiek** operacje wykonywane na danych osobowych, takie jak zbieranie (np. przyjmowanie dokumentów), utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, zarówno w zbiorach tradycyjnych (papierowych), jak i w systemach informatycznych,
6. niszczenie (usuwanie) danych – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
7. osoba upoważniona do przetwarzania danych osobowych – pracownik Uniwersytetu lub podmiotu zewnętrznego, który został przeszkolony w zakresie ochrony danych osobowych i uzyskał upoważnienie do ich przetwarzania,
8. dysponent danych – osoba fizyczna, której dotyczą dane,
9. osoba nieuprawniona – osoba niezatrudniona przy przetwarzaniu danych osobowych (z wyłączeniem osoby uprawnionej do ich przeglądania i przetwarzania na mocy odrębnych przepisów).

II. Zasady dopuszczania osób do przetwarzania danych osobowych

§ 3

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych (Rektora).
2. Upoważnienia do przetwarzania danych osobowych nadaje w imieniu Rektora Administrator Bezpieczeństwa Informacji.

§ 4

1. Upoważnienie nadawane jest na pisemny wniosek bezpośredniego przełożonego upoważnianej osoby, przedkładany Administratorowi Bezpieczeństwa Informacji. Wniosek powinien zawierać w szczególności: nazwisko i imię pracownika, nazwę stanowiska pracy, opis stanowiska lub zakresu obowiązków związanych z przetwarzaniem danych osobowych, określenie wnioskowanego zakresu danych osobowych i sposobu ich przetwarzania oraz uzasadnienie wniosku.
2. W przypadku osoby wykonującej na podstawie umowy cywilno-prawnej usługę, w ramach której przetwarzane są dane osobowe (zwanej dalej „osobą współpracującą z Uniwersytetem"), z wnioskiem o nadanie upoważnienia występuje kierownik jednostki organizacyjnej zlecającej usługę. Wniosek powinien zawierać w szczególności: nazwisko i imię osoby wykonującej usługę, określenie zakresu wykonywanych w ramach usługi czynności związanych z przetwarzaniem danych osobowych, określenie wnioskowanego zakresu danych osobowych i sposobu ich przetwarzania, uzasadnienie wniosku oraz, jeśli jest znany, termin zakończenia usługi.
3. Administrator Bezpieczeństwa Informacji zobowiązany jest rozpatrzyć wniosek

w terminie 5 dni od dnia jego otrzymania. W szczególnych przypadkach termin ten może ulec wydłużeniu.

4. Administrator Bezpieczeństwa Informacji może:
   1) wyrazić zgodę na nadanie uprawnień zgodnie z wnioskowanym zakresem,
   2) wyrazić zgodę na nadanie ograniczonych uprawnień zawierających się we wnioskowanym zakresie,
   3) nie wyrazić zgody na nadanie uprawnień.
5. Decyzję Administrator Bezpieczeństwa Informacji przekazuje osobie wnioskującej. W przypadku wydania decyzji o ograniczeniu uprawnień lub odmowy wydania upoważnienia, decyzja musi być sporządzona w formie pisemnej i zawierać uzasadnienie. Od decyzji Administratora Bezpieczeństwa Informacji wnioskujący może odwołać się do Rektora. Decyzja Rektora jest ostateczna.
6. Osoba wnioskująca przekazuje decyzję Administratora Bezpieczeństwa Informacji pracownikowi.

§ 5

1. Nadanie upoważnienia do przetwarzania danych osobowych (w szczególności w systemie informatycznym) obejmuje:
   1) przeprowadzenie przez Administratora Bezpieczeństwa Informacji szkolenia w zakresie bezpieczeństwa danych osobowych oraz prawnych aspektów ochrony tych danych,
   2) wydanie przez Administratora Bezpieczeństwa Informacji pisemnego upoważnienia pracownika do przetwarzania danych osobowych, zawierającego zakres nadawanych uprawnień do przetwarzania danych osobowych, informację o zbiorze osób, do którego nadawane są uprawnienia, systemie informatycznym, w którym dane będą przetwarzane (jeśli dotyczy), datę nadania upoważnienia oraz, jeśli upoważnienie nadawane jest terminowo, datę wygaśnięcia upoważnienia,
   3) w przypadku przetwarzania danych osobowych w systemie informatycznym - nadanie pracownikowi przez administratora systemu informatycznego identyfikatora oraz hasła, a także skonfigurowanie uprawnień w systemie.
2. W przypadku konieczności zmiany zakresu upoważnienia (inny lub kolejny zbiór osób, inny zakres przetwarzania danych osobowych, zmiana stanowiska pracy przez pracownika) należy przedłożyć Administratorowi Bezpieczeństwa Informacji nowy wniosek o nadanie upoważnienia, stosując odpowiednio zapisy § 4.
3. W przypadku nadania nowego upoważnienia, moc traci poprzednie upoważnienie.

§ 6

1. Odebranie upoważnienia do przetwarzania danych osobowych może mieć miejsce, gdy:

1) z pracownikiem została rozwiązana (zakończona) umowa o pracę,

2) zakres obowiązków służbowych pracownika uległ zmianie, która spowodowała utratę potrzeby przetwarzania danych osobowych,

3) pracownik spowodował swoim celowym działaniem incydent mający negatywny wpływ na bezpieczeństwo przetwarzanych danych osobowych,

4) istnieje uzasadniona obawa, że przetwarzanie danych osobowych przez pracownika wiąże się z poważnym ryzykiem utraty poufności, integralności lub dostępności tych danych.

2. Odebranie uprawnień może nastąpić na wniosek:

1) Rektora,

2) przełożonego pracownika,

3) kierownika Działu Kadr i Szkolenia,

4) Administratora Bezpieczeństwa Informacji.

3. Proces odebrania upoważnienia obejmuje:

1) przekazanie Administratorowi Bezpieczeństwa Informacji pisemnego wniosku o odebranie upoważnienia (za wyjątkiem sytuacji, gdy wnioskującym jest Administrator Bezpieczeństwa Informacji) z określeniem imienia i nazwiska pracownika oraz jego identyfikatora w systemie informatycznym (jeśli pracownik posiada dostęp do systemu informatycznego), a także przyczyny konieczności odebrania upoważnienia,

2) w przypadku posiadania przez pracownika, któremu upoważnienie jest odbierane uprawnień do systemu informatycznego, przekazanie przez Administratora Bezpieczeństwa Informacji administratorowi systemu informatycznego polecenia unieważnienia hasła, zablokowania konta użytkownika, odebrania wszelkich uprawnień do systemu; administrator systemu winien możliwie szybko wykonać niezbędne czynności,

3) poinformowanie przez Administratora Bezpieczeństwa Informacji wnioskodawcy o odebraniu pracownikowi upoważnienia do przetwarzania danych osobowych i o odebraniu (jeśli nastąpiło) uprawnień do systemu informatycznego.

§ 7

1. Upoważnienie do przetwarzania danych osobowych przygotowywane jest w dwóch egzemplarzach: oryginał dla upoważnianego pracownika, a kopia dla Administratora Bezpieczeństwa Informacji. W przypadku udzielania upoważnienia osobie nie będącej pracownikiem Uczelni (będącej np. pracownikiem podmiotu zewnętrznego współpracującego z Uczelnią przy przetwarzaniu danych osobowych), przygotowywana jest druga kopia upoważnienia, przechowywana w jednostce zlecającej przetwarzanie danych (występującej z wnioskiem o udzielenie upoważnienia).
2. Administrator Bezpieczeństwa Informacji prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych, obejmującą: imię i nazwisko pracownika, datę nadania upoważnienia, datę ustania upoważnienia,

zakres upoważnienia, identyfikator użytkownika w systemie informatycznym.

§ 8

1. Pracownicy nieposiadający w zakresie swoich obowiązków czynności związanych z przetwarzaniem danych osobowych (osoby sprzątające, portierzy, pracownicy techniczni, konserwatorzy, elektrycy itp.), a których obowiązki wymuszają pracę - pod nieobecność osób upoważnionych do przetwarzania danych osobowych - w pomieszczeniach, w których dane osobowe są przetwarzane, muszą zostać zapoznane z zasadami dotyczącymi ochrony danych osobowych oraz uzyskać upoważnienie do przebywania w w/w pomieszczeniach.

III. Szkolenia w zakresie bezpieczeństwa danych osobowych

§ 9

1. Przed dopuszczeniem do przetwarzania danych osobowych pracownik Uniwersytetu (lub osoba współpracująca z Uniwersytetem) musi zostać przeszkolony w zakresie przepisów prawnych dotyczących ochrony danych osobowych oraz zasad ochrony danych osobowych obowiązujących w Uniwersytecie. Za przeprowadzenie szkolenia odpowiada Administrator Bezpieczeństwa Informacji, a za jego zorganizowanie odpowiada przełożony szkolonego pracownika.
2. Szkolenie w szczególności powinno obejmować:
   1) przedstawienie Ustawy o ochronie danych osobowych i jej wpływu na przebieg procesów związanych z przetwarzaniem danych osobowych w Uniwersytecie,
   2) przedstawienie Rozporządzenia Ministra Spraw Wewnętrznych i Administracji,
   3) przedstawienie przepisów wewnętrznych obowiązujących w Uniwersytecie, regulujących zasady ochrony danych osobowych,
   4) przedstawienie praktycznych rozwiązań ochrony danych osobowych na danym stanowisku pracy.
3. Po odbytym szkoleniu bezpośredni przełożony pracownika (lub w przypadku osoby współpracującej z Uniwersytetem, kierownik jednostki zlecającej usługę) może wystąpić do Administratora Bezpieczeństwa Informacji z wnioskiem o nadanie pracownikowi (osobie współpracującej) upoważnienia do przetwarzania danych osobowych.
4. Oprócz szkolenia określonego w ust. 1 i 2, w poszczególnych jednostkach organizacyjnych prowadzone być powinny w miarę możliwości szkolenia okresowe (powtórzeniowe) oraz szkolenia przedstawiające zmiany w przepisach o ochronie danych osobowych lub zmiany zasad ochrony danych osobowych obowiązujących w Uniwersytecie.

IV. Zasady obowiązujące przy zbieraniu danych

§ 10

1. Każda osoba, której dane osobowe są lub mają być przetwarzane

w Uniwersytecie **musi zostać poinformowana** przez administratora danych (Uniwersytet) o adresie siedziby Uniwersytetu i jego pełnej nazwie, celu zbierania danych oraz ich potencjalnych odbiorcach, o prawie dostępu osoby do treści swoich danych oraz ich poprawiania, jak również o obowiązku (lub jego braku) podania przez osobę danych i jeśli obowiązek występuje, o jego podstawie prawnej. Informacji należy udzielić przed uzyskaniem od osoby jej danych, umieszczając w kwestionariuszu osobowym (lub w innej formie) odpowiednią treść informacji.

2. W przypadku aktualnie zatrudnionych pracowników oraz kandydatów na pracowników oświadczenie o poinformowaniu osoby przez Uniwersytet o okolicznościach wskazanych w ust. 1. wraz z podpisem pracownika (kandydata na pracownika) przyjmuje Dział Kadr i Szkolenia. Dokument tworzony jest w jednym egzemplarzu, przechowywanym w aktach osobowych pracownika.
3. W przypadku kandydatów na studia informacja o okolicznościach wskazanych w ust. 1. umieszczona musi być na pierwszej stronie rejestracji internetowego systemu rekrutacji. By przejść do kolejnych etapów rejestracji, kandydat musi potwierdzić, że został o w/w okolicznościach poinformowany. Oświadczenie (potwierdzenie o poinformowaniu) przechowywane jest w formie elektronicznej.
4. W przypadku studentów, doktorantów oraz innych osób kształcących się w Uniwersytecie oświadczenie o poinformowaniu osoby przez Uniwersytet o okolicznościach wskazanych w punkcie 1. wraz z podpisem osoby kształcącej się przyjmuje jednostka prowadząca rekrutację. Dokument tworzony jest w jednym egzemplarzu, przechowywanym w teczce osobowej.

V. Zasady ochrony danych osobowych

§ 11

1. Osoby upoważnione do przetwarzania danych osobowych przetwarzają je tylko w zakresie wynikającym z udzielonego im upoważnienia.
2. Przetwarzający dane zobowiązani są do zachowania w tajemnicy treści przetwarzanych danych oraz sposobów ich zabezpieczania.

§ 12

1. Zabronione jest wywieszanie w miejscach ogólnodostępnych (np. gablotach na korytarzach) jakichkolwiek list lub innych dokumentów zawierających dane osobowe. Wyjątkiem są przypadki wynikające z przepisów prawa określających jawność danego procesu (np. listy z wynikami rekrutacji na studia, wyniki przetargów w ramach zamówień publicznych, w których zwycięzcami są osoby fizyczne).
2. Dopuszczalne jest wywieszanie w miejscach ogólnodostępnych list studentów z podziałem na grupy ćwiczeniowe, laboratoryjne itp. Jednak na listach mogą zostać podane wyłącznie imię i nazwisko studenta. Niedopuszczalne jest podawanie na takich listach jakichkolwiek innych danych osobowych (np. adresu, numeru PESEL, daty urodzenia itd.).
3. Zabronione jest przekazywanie danych osobowych osobom

nieuprawnionym telefonicznie, elektronicznie lub w jakiejkolwiek innej formie.

4. Przekazywanie w ramach jednostki organizacyjnej lub pomiędzy jednostkami nośników informatycznych lub dokumentów zawierających dane osobowe, może odbywać się tylko pomiędzy osobami posiadającymi upoważnienia do przetwarzania danych osobowych określonych zbiorów osób.

5. Pracowników przetwarzających dane osobowe obowiązuje zasada „czystego biurka", a więc niepozostawianie „na wierzchu", w szczególności w miejscu dostępnym dla osób nieuprawnionych, niezabezpieczonych dokumentów oraz nośników zawierających dane osobowe.

6. Osoby nieuprawnione mogą przebywać w pomieszczeniu, w którym przetwarzane są dane osobowe jedynie w obecności pracownika Uniwersytetu upoważnionego do przetwarzania tych danych.

7. Klucze oraz uprawnienia (na przykład kody alarmu) do pomieszczeń, w których przetwarzane są dane osobowe, mogą być udostępniane jedynie osobom upoważnionym do przetwarzania danych osobowych lub osobom posiadającym upoważnienie do przebywania w takich pomieszczeniach.

§ 13

1. Użytkownik systemu informatycznego nie może udostępniać identyfikatora, hasła i stanowiska roboczego innym osobom, w szczególności osobom nieuprawnionym.

2. Zabronione jest zapisywanie hasła w sposób umożliwiający dostęp do niego innym osobom.

3. W jednostkach organizacyjnych i systemach informatycznych, w których jest to możliwe, należy użytkownikom ograniczyć uprawnienia czasowe do pracy w godzinach roboczych.

4. Podłączenie urządzenia końcowego (komputera, terminala, drukarki) do sieci informatycznej Uniwersytetu dokonywane jest przez administratora systemu informatycznego (sieci) lub osobę przez niego wyznaczoną.

5. Monitory stanowisk komputerowych, na których przetwarzane są dane osobowe, znajdujące się w pomieszczeniach, w których mogą przebywać osoby nieuprawnione, należy ustawić w taki sposób, aby uniemożliwić tym osobom wgląd w dane.

6. Niedozwolone jest przesyłanie danych osobowych lub dokumentów je zawierających z wykorzystaniem kont pocztowych spoza domeny *ukw.edu.pl* – zarówno w przypadku nadawcy, jak i odbiorcy.

7. Serwis sprzętu komputerowego zawierającego dane osobowe wykonywany jest wyłącznie przez pracowników Działu Informatyzacji. Jeśli zaistnieje konieczność przekazania takiego sprzętu do serwisu zewnętrznego, bezwzględnie należy z przekazywanych twardych dysków i innych nośników informatycznych usunąć dane osobowe w sposób uniemożliwiający ich odczyt.

8. Serwery lub inne istotne dla przetwarzania danych osobowych elementy systemów informatycznych nie mogą być umieszczane bezpośrednio na podłodze ze względu na możliwość zniszczenia przez wodę w przypadku awarii

sieci wodociągowej i zalania pomieszczenia. Serwerownie muszą być także wyposażone w odpowiedni sprzęt gaśniczy.

9. Serwery systemów informatycznych, w których przetwarzane są dane osobowe oraz inne urządzenia informatyczne przechowujące te dane muszą być zabezpieczone przed nieprzewidzianymi przerwami w zasilaniu przy pomocy zasilaczy awaryjnych (UPS). Jeśli istnieje taka możliwość, również inne komputery, przy pomocy których przetwarzane są dane osobowe, powinny być zabezpieczone przy pomocy zasilaczy awaryjnych.

10. Komputery oraz inne urządzenia informatyczne, przy pomocy których przetwarzane są dane osobowe, powinny posiadać wydzielony obwód zasilania, dedykowany dla sprzętu informatycznego. Szczególnie niedopuszczalne jest zasilanie z tych samych gniazd, listew zasilających lub przeciwprzepięciowych urządzeń o dużym poborze mocy (na przykład czajników elektrycznych, grzejników itp.).

11. W przypadku planowanych wyłączeń zasilania/energii elektrycznej, pracownicy działu przeprowadzającego wyłączenie muszą o nim bezwzględnie poinformować odpowiednio wcześniej wszystkie jednostki organizacyjne, których wyłączenie może dotyczyć, a w których dane osobowe przetwarzane są z wykorzystaniem systemów informatycznych, tak by przed wyłączeniem zasilania można było w bezpieczny sposób zakończyć przetwarzanie danych w systemie.

§ 14

1. Dane osobowe przetwarzane w systemie informatycznym muszą być zabezpieczane poprzez tworzenie kopii zapasowych umożliwiających odtworzenie danych w przypadku awarii. Za wykonywanie kopii odpowiadają administratorzy systemów informatycznych lub osoby wyznaczone do zarządzania systemem (na przykład w przypadku pozasieciowych, jednostanowiskowych systemów).

2. Kopie zapasowe tworzone na zewnętrznych nośnikach informatycznych (na taśmach, pendrive'ach, płytach CD, DVD, dyskietkach itp.) muszą być przechowywane w szafach, szufladach lub pomieszczeniach, zamykanych na klucz, do których dostęp mają jedynie osoby odpowiedzialne za wykonywanie i zabezpieczanie tych kopii. Należy je przechowywać w innym pomieszczeniu (a w miarę możliwości innym budynku), niż to, w którym znajduje się (na przykład na serwerze) oryginalny, wykorzystywany w bieżącej pracy zbiór danych.

3. Dane osobowe wykorzystywane poza systemem informatycznym (na pendrive'ach, płytach CD, DVD, dyskietkach itp.) po zakończeniu pracy muszą być przechowywane w zamykanych na klucz meblach biurowych. Klucze do mebli należy zabezpieczyć przed dostępem osób nieupoważnionych do przetwarzania danych osobowych

4. W komputerach, w których nie ma potrzeby wykorzystywania zewnętrznych nośników danych (pendrive'ów, dyskietek, płyt CD-R/DVD-R itp.) należy w miarę możliwości zablokować napęd dyskietek, możliwość zapisu na płytach CD-R/DVD-R oraz porty USB, by ograniczyć możliwość kopiowania danych osobowych na takie nośniki.

5. Dokumenty w formie papierowej zawierające dane osobowe winny być przechowywane w szafach zamykanych na klucz, do których dostęp mają

jedynie osoby upoważnione do przetwarzania danych osobowych.

6. Jeśli przechowywanie dokumentów w formie papierowej w szafach nie jest możliwe, należy uniemożliwić dostęp do tych dokumentów osobom nieupoważnionym, przy czym dokumenty nie mogą być przechowywane na podłodze, ze względu na możliwość zniszczenia ich przez wodę w przypadku awarii sieci wodociągowej i zalania pomieszczenia.

7. Robocze, błędne lub nieaktualne wydruki oraz kopie danych tworzone na nośnikach informatycznych należy usuwać (niszczyć) natychmiast po ustaniu ich przydatności.

8. Niedopuszczalne jest pozostawianie po zakończeniu pracy w danym dniu dokumentów, wydruków zawierających dane osobowe w drukarkach, kserokopiarkach i tym podobnych urządzeniach.

9. Niepotrzebne już dokumenty w formie papierowej zawierające dane osobowe muszą zostać zniszczone w sposób uniemożliwiający ich odczytanie, najlepiej przy pomocy niszczarki. **Nie wolno wyrzucać takich dokumentów bez odpowiedniego ich zniszczenia!**

10. **Zabronione jest wynoszenie poza obiekty Uniwersytetu danych osobowych w jakiejkolwiek formie, zarówno papierowej, jak i elektronicznej**. Wyjątkiem są sytuacje wymagające przekazania danych osobowych pomiędzy jednostkami organizacyjnymi Uniwersytetu znajdującymi się w różnych lokalizacjach.

11. Pomieszczenia zawierające kluczowe z punktu widzenia ochrony danych osobowych zbiory, jak archiwa lub serwerownie, należy w miarę możliwości zabezpieczyć dodatkowo poprzez instalację zamków wyższej klasy, systemów alarmowych i krat w oknach (jeśli pomieszczenie posiada okna). Pomieszczenia takie muszą być całodobowo nadzorowane przez pracowników ochrony bezpośrednio lub z wykorzystaniem, o ile to możliwe, systemu monitoringu.

VI. Udostępnianie danych osobowych

§ 15

1. Uniwersytet udostępnia przetwarzane dane osobowe wyłącznie osobom do tego upoważnionym na mocy uregulowań wewnętrznych obowiązujących w tym zakresie na jego obszarze.

2. Upoważnienie, o którym mowa w ust. 1., wynikać może w szczególności:

   1) z charakteru pracy wykonywanej na danym stanowisku pracy,

   2) z dokumentu określającego zakres obowiązków (zakres czynności) wykonywanych na danym stanowisku pracy,

   3) z odrębnego dokumentu zawierającego imienne upoważnienie do dostępu do danych osobowych.

3. Uniwersytet zapewnia dostęp do przetwarzanych danych osobowych osobom fizycznym będącym dysponentami tych danych.

4. Dysponentami danych osobowych są osoby, które powierzyły swoje dane Uniwersytetowi.

5. Osoby niezatrudnione przy przetwarzaniu danych osobowych określonej kategorii, w tym dysponenci danych osobowych, osoby mające interes prawny w uzyskaniu dostępu do tych danych mogą mieć do nich **wgląd wyłącznie** w obecności upoważnionego pracownika Uniwersytetu.

6. Dostęp do danych osobowych i ich przetwarzanie bez odrębnego upoważnienia administratora danych osobowych (Rektora) lub upoważnionej przezeń osoby (Administratora Bezpieczeństwa Informacji) może mieć miejsce wyłącznie w przypadku działań podmiotów upoważnionych na mocy odpowiednich przepisów prawa do dostępu i przetwarzania danych określonej kategorii.

7. W szczególności dostęp do danych osobowych na wskazanej w ust. 6. zasadzie mogą mieć: Państwowa Inspekcja Pracy, Zakład Ubezpieczeń Społecznych, organy skarbowe, Policja, Straż Graniczna, Służba Celna, Żandarmeria Wojskowa, Agencja Bezpieczeństwa Wewnętrznego, prokuratura, sądy powszechne, Najwyższa Izba Kontroli, Generalny Inspektor Ochrony Danych Osobowych i inne upoważnione przez przepisy prawa podmioty i organy, działające w granicach przyznanych im uprawnień - wszystkie w/w po okazaniu dokumentów potwierdzających te uprawnienia.

8. **W przypadku studentów**, na podstawie § 10, ust.4 rozporządzenia Ministra Nauki i Szkolnictwa Wyższego w sprawie dokumentacji przebiegu studiów z dnia 2 listopada 2006 roku (Dz.U. 2006 Nr 224, poz. 1634), **udostępnianie dokumentacji oraz informacji dotyczących przebiegu studiów osobom innym, niż student lub osoba upoważniona przez niego na piśmie, jest niedozwolone**.

§ 16

1. Dysponent danych osobowych (osoba, której dane są przetwarzane) może upoważnić inną osobę do odbioru jej danych osobowych. Upoważnienie musi być sporządzone w formie pisemnej. Upoważnienie takie przechowywane jest bezterminowo przez jednostkę organizacyjną udostępniającą dane osobowe.

2. Pracownik Uniwersytetu udostępniający dane na podstawie takiego upoważnienia ma obowiązek potwierdzić tożsamość osoby, której udostępnia się te dane.

VII. Powierzanie przetwarzania danych osobowych

§ 17

1. W przypadku przekazywania danych osobowych, których administratorem jest Uniwersytet, do przetwarzania podmiotom zewnętrznym konieczne jest zawarcie z podmiotem zewnętrznym pisemnej umowy o powierzeniu przez Uniwersytet przetwarzania danych osobowych. Może to być odrębna umowa lub integralna część umowy pierwotnej (umowy, z której wynika konieczność przekazania danych osobowych).

2. Umowę przygotowuje jednostka organizacyjna powierzająca przetwarzanie danych osobowych, we współpracy z Radcą Prawnym Uniwersytetu oraz Administratorem Bezpieczeństwa Informacji.

3. Warunki umowy dotyczące ochrony powierzanych danych osobowych akceptuje Administrator Bezpieczeństwa Informacji.

4. Umowa musi w szczególności określać zakres oraz cel przetwarzania danych przez podmiot, któremu dane powierzono oraz zobowiązywać podmiot przed rozpoczęciem przetwarzania danych do podjęcia środków zabezpieczających dane, o których mowa w art. 36-39 Ustawy oraz do spełnienia wymagań określonych w art. 39a Ustawy, a więc:

   1) sporządzenia wymaganej dokumentacji podobnie, jak administrator danych (polityka bezpieczeństwa, instrukcja zarządzania systemem informatycznym, w którym przetwarzane będą powierzane dane),

   2) należytego zabezpieczenia systemu informatycznego przed ingerencją osób trzecich lub innych nieuprawnionych podmiotów,

   3) należytego zabezpieczenia danych osobowych,

   4) prowadzenia ewidencji osób uprawnionych do przetwarzania powierzanych danych osobowych.

5. W uzasadnionych wypadkach Administrator Bezpieczeństwa Informacji może nie wyrazić zgody na powierzenie przetwarzania danych osobowych podmiotowi zewnętrznemu.

VIII. Zasady rejestracji zbiorów danych

§ 18

1. Zgodnie z przepisami Ustawy o ochronie danych osobowych administrator danych (Uniwersytet) ma w szczególnych przypadkach obowiązek zarejestrowania prowadzonych zbiorów danych osobowych dla danej kategorii osób. W przypadku tworzenia przez jednostkę organizacyjną zbioru dla nowej kategorii osób, zobowiązuje się kierownika jednostki do dokonania wraz z Administratorem Bezpieczeństwa Informacji ustaleń w zakresie konieczności rejestracji zbiorów danych osobowych. Ustaleń tych należy dokonać przed utworzeniem zbioru.

2. W przypadku konieczności rejestracji zbioru, kierownik jednostki tworzącej zbiór zobowiązany jest do przekazania Administratorowi Bezpieczeństwa Informacji wszelkich informacji niezbędnych do rejestracji zbioru.

§ 19

1. Kierownik jednostki organizacyjnej, w której wykorzystywany jest zarejestrowany zbiór, zobowiązany jest do informowania Administratora Bezpieczeństwa Informacji o wszelkich zmianach dotyczących zbioru, mogących powodować konieczność modyfikacji zgłoszenia zbioru jak również o zakończeniu przetwarzania danych osobowych w zbiorze.

2. Okoliczności, o których mowa w ust. 1, winny być zgłoszone Administratorowi Bezpieczeństwa Informacji, który dokonuje rejestracji lub wyrejestrowania zbiorów oraz zgłasza zmiany w zbiorach w biurze Generalnego Inspektora Ochrony Danych Osobowych, w możliwie krótkim terminie.

IX. Opis zdarzeń naruszających ochronę danych osobowych oraz zasady postępowania w sytuacji naruszenia ochrony danych osobowych

§ 20

1. Rodzaje zagrożeń naruszających ochronę danych osobowych:

   1) zagrożenia losowe:

      a) zewnętrzne (np. klęski żywiołowe, pożary, zalania, przerwy w zasilaniu energii) – ich wystąpienie może prowadzić do utraty integralności danych lub ich zniszczenia (zarówno danych przetwarzanych w formie tradycyjnej papierowej, jak i elektronicznej) lub uszkodzenia infrastruktury technicznej systemu informatycznego, przy czym ciągłość pracy systemu zostaje zakłócona, jednak nie dochodzi do naruszenia poufności danych;

      b) wewnętrzne (np. niezamierzone pomyłki użytkowników, administratora, awarie sprzętowe, błędy oprogramowania) – w wyniku ich wystąpienia może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu informatycznego, może nastąpić naruszenie poufności danych;

   2) zagrożenia zamierzone (świadome i celowe naruszenia poufności danych) – w wyniku ich wystąpienia zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy; w ramach tej kategorii zagrożeń wyróżnia się:

      a) nieuprawniony dostęp do systemu informatycznego z zewnątrz (włamanie do systemu),

      b) nieuprawniony dostęp do systemu informatycznego z jego wnętrza,

      c) nieuprawnione przekazanie danych,

      d) bezpośrednie zagrożenie materialnych składników (np. kradzież sprzętu informatycznego zawierającego dane osobowe, kradzież dokumentów).

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

   1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu (np. wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej);

   2) niewłaściwe parametry środowiska (np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych);

   3) awarie sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych;

   4) pojawienie się odpowiedniego komunikatu alarmowego od części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;

   5) pogorszenie jakości danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu informatycznego lub inną

nadzwyczajną i niepożądaną modyfikację w systemie;

6) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie;

7) modyfikacja danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia;

8) ujawnienie osobom nieuprawnionym danych osobowych lub objętych tajemnicą procedur ochrony ich przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń (np. identyfikatora i hasła w systemie informatycznym);

9) praca w systemie informatycznym, wykazująca 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, sygnał o uporczywym nieautoryzowanym logowaniu);

10) podmienienie albo zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub skasowanie bądź skopiowanie w sposób niedozwolony danych osobowych;

11) rażące naruszenie obowiązków w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce lub kserokopiarce, wyrzucenie do śmieci dokumentów w formie papierowej niezniszczonych w sposób uniemożliwiający odczytanie danych, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii zapasowych, prace na danych osobowych w celach prywatnych, itp.)

3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych znajdujących się na dyskach, dyskietkach, pamięciach flash, płytach CD, DVD, taśmach magnetycznych, kartach pamięci itp. oraz wydrukach komputerowych oraz wszelkie stwierdzone nieprawidłowości w zakresie zabezpieczenia fizycznego miejsc przechowywania i przetwarzania danych osobowych (niezabezpieczone pomieszczenia, otwarte szafy, biurka, regały, urządzenia archiwizujące, dokumenty pozostawione w drukarkach, kserokopiarkach, niezniszczone w odpowiedni sposób dokumenty w śmietnikach itp.).

§ 21

1. Każdy pracownik (w szczególności osoba zatrudniona przy przetwarzaniu danych osobowych), który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych przetwarzanych w Uniwersytecie zobowiązany jest do niezwłocznego poinformowania o tym swojego przełożonego, a ten do poinformowania administratora systemu informatycznego, jeśli zdarzenie dotyczy systemu informatycznego oraz Administratora Bezpieczeństwa Informacji Uniwersytetu.

2. Administrator systemu informatycznego, który stwierdził lub uzyskał informację wskazującą na naruszenie w systemie ochrony danych osobowych zobowiązany jest do niezwłocznego:

1) zapisania wszelkich informacji i okoliczności związanych z danym zdarzeniem, a w szczególności dokładnego czasu uzyskania informacji o naruszeniu ochrony danych osobowych lub samodzielnym wykryciu tego faktu,

2) jeżeli zasoby systemu na to pozwalają, wygenerowania i wydrukowania wszystkich dokumentów i raportów, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzenia ich datą i podpisania,

3) przystąpienia do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym do określenia skali zniszczeń, metody dostępu osoby niepowołanej do danych itp.,

4) podjęcia odpowiednich kroków w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych, w tym między innymi:

   a) fizycznego odłączenia urządzeń i segmentów sieci które mogły umożliwić dostęp do bazy danych osobie niepowołanej,

   b) wylogowania użytkownika podejrzanego o naruszenie ochrony danych,

   c) zmianę hasła użytkownika, poprzez którego uzyskano nielegalny dostęp, w celu uniemożliwienia ponownej skutecznej próby uzyskania takiego dostępu,

5) szczegółowej analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych,

6) przywrócenia normalnego działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, odtworzenia jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności mających na celu uniknięcie ponownego uzyskania dostępu przez osobę nieupoważnioną w ten sam sposób.

4. Po przywróceniu normalnego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia, oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

5. Jeżeli przyczyną zdarzenia był błąd użytkownika systemu informatycznego, należy przeprowadzić ponowne szkolenie w zakresie ochrony danych osobowych w systemie informatycznym.

6. Jeżeli przyczyną zdarzenia była infekcja wirusem, należy ustalić źródło jego pochodzenia i wykonać zabezpieczenia antywirusowe i organizacyjne wykluczające powtórzenie się podobnego zdarzenia w przyszłości.

7. Jeżeli przyczyną zdarzenia było zaniedbanie ze strony użytkownika systemu należy wyciągnąć konsekwencje dyscyplinarne wynikające z kodeksu pracy oraz ustawy o ochronie danych osobowych.

8. Administrator bazy danych osobowych (np. administrator systemu informatycznego), w której nastąpiło naruszenie ochrony danych osobowych przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia i w terminie 14 dni od daty jego zaistnienia przekazuje Administratorowi Bezpieczeństwa Informacji Uniwersytetu.

9. Administrator Bezpieczeństwa Informacji Uniwersytetu przeprowadza analizę raportu i stosownie do sytuacji rekomenduje do realizacji odpowiednie działania mające na celu zabezpieczenie przed ponownym wystąpieniem zdarzenia w przyszłości.

X. Postanowienia końcowe

§ 22

Polityka bezpieczeństwa przetwarzania danych osobowych w Uniwersytecie Kazimierza Wielkiego wchodzi w życie z dniem 01.05.2013 roku.

Załącznik Nr 2
do Zarządzenia Nr 68/2012/2013
Rektora UKW z dnia 29.04.2013 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI służącymi do przetwarzania danych osobowych w Uniwersytecie Kazimierza Wielkiego

Rozdział 1
Postanowienia ogólne

1. Instrukcja zarządzania systemami informatycznymi, zwana dalej „Instrukcją", określa procedury dotyczące zasad pracy i zachowania bezpieczeństwa w systemach informatycznych wykorzystywanych w Uniwersytecie Kazimierza Wielkiego, jak również przetwarzania w nich danych osobowych.
2. Instrukcja została opracowana zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późń. zm.), zwaną dalej „ustawą o ochronie danych osobowych" oraz rozporządzeniem 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. z 2004 r. Nr 100, poz. 1024).
3. Możliwe jest wprowadzanie szczegółowych instrukcji lub polityk bezpieczeństwa dotyczących poszczególnych systemów informatycznych. W takim przypadku zapisy instrukcji (polityk) szczegółowych są nadrzędne w stosunku do zapisów niniejszej instrukcji, jednak nie mogą one ustanawiać niższego poziomu zabezpieczeń, niż niniejsza instrukcja.
4. Dla każdego wielostanowiskowego systemu informatycznego musi zostać wyznaczony przynajmniej jeden administrator systemu, posiadający między innymi uprawnienia do tworzenia w systemie kont użytkowników i nadawania im uprawnień.

Rozdział 2

Nadawanie uprawnień do przetwarzania danych osobowych oraz ich rejestrowanie w systemie informatycznym

1. Przed dopuszczeniem do pracy w systemach informatycznych oraz do pracy przy przetwarzaniu danych osobowych, każdy użytkownik powinien zostać zapoznany przez przełożonego, administratora systemu lub administratora bezpieczeństwa informacji z zasadami obowiązującymi podczas pracy w systemach informatycznych, przepisami dotyczącymi ochrony danych osobowych oraz obowiązującymi w Uniwersytecie wewnętrznymi regulacjami w tym zakresie.
2. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład służących do przetwarzania danych osobowych mogą zostać dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych wydane przez administratora bezpieczeństwa informacji.
3. Wydanie upoważnienia oraz rejestracja użytkownika w systemie informatycznym przetwarzającym dane osobowe następuje na wniosek przełożonego użytkownika.
4. Jeżeli osoba mająca przetwarzać dane osobowe nie jest pracownikiem Uczelni, z wnioskiem o wydanie dla niej upoważnienia występuje kierownik jednostki zlecającej upoważnianej osobie przetwarzanie danych osobowych.
5. Procedury wydawania i odwoływania upoważnień do przetwarzania danych osobowych realizowane są według następujących zasad:
   1) przełożony użytkownika lub kierownik jednostki, o którym mowa w ust. 4, składa do administratora bezpieczeństwa informacji pisemny wniosek o wydanie upoważnienia, który zawiera:
      a) imię i nazwisko użytkownika (osoby upoważnianej),
      b) w przypadku pracownika Uczelni, stanowisko zajmowane przez użytkownika,
      c) nazwę zbioru danych osobowych oraz nazwę systemu informatycznego, do którego użytkownik ma uzyskać dostęp,
      d) zakres upoważnienia do przetwarzania danych osobowych,
      e) datę, z jaką upoważnienie ma być wydane,
      f) okres ważności upoważnienia lub informację o jego bezterminowości,

2) administrator bezpieczeństwa informacji ma prawo odmówić wydania upoważnienia; informuje wtedy wnioskodawcę w formie pisemnej o powodach odmowy,
3) w przypadku udzielenia upoważnienia, jego oryginał zostaje przekazany upoważnianemu użytkownikowi, a kopia zostaje włączona do wykazu prowadzonego przez administratora bezpieczeństwa informacji.
4) po udzieleniu upoważnienia do przetwarzania danych osobowych, administrator systemu informatycznego nadaje użytkownikowi uprawnienia do systemu,
5) jeżeli dane osobowe przetwarzane są poza systemem informatycznym (sieciowym), jednostanowiskowo, identyfikator i hasło dostępu do bazy danych ustala użytkownik,
6) wyrejestrowania użytkownika z systemu informatycznego (pozbawienia dostępu do systemu) dokonuje, na wniosek administratora bezpieczeństwa informacji lub przełożonego użytkownika, administrator systemu informatycznego.

6. Przyznanie uprawnień do przetwarzania danych osobowych w systemie informatycznym polega na wprowadzeniu do systemu przez jego administratora dla użytkownika unikatowego identyfikatora, hasła oraz ustanowienia zakresu dostępnych danych i operacji, przy czym o brzmieniu identyfikatora administrator systemu informuje administratora bezpieczeństwa informacji.
7. Za przydzielenie identyfikatora i wygenerowanie hasła użytkownikowi, który po raz pierwszy korzysta z systemu informatycznego, odpowiada administrator systemu. Późniejsze cykliczne zmiany hasła muszą być wymuszane automatycznie poprzez mechanizmy zawarte w systemie informatycznym lub poprzez działanie administratora systemu.
8. Jeżeli dane osobowe przetwarzane są poza systemem informatycznym (sieciowym), za zmianę hasła odpowiada użytkownik.
9. Identyfikator użytkownika nie może być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego (zamknięciu dostępu do systemu), nie może być przydzielany innej osobie. W przypadku wyrejestrowania użytkownika z systemu, administrator systemu pozostawia w systemie identyfikator i zmienia hasło dostępu.
10. Przełożeni użytkowników lub kierownicy jednostek organizacyjnych, o których mowa w ust. 4, zobowiązani są pisemnie informować administratora

bezpieczeństwa informacji o każdej zmianie dotyczącej użytkowników, mającej wpływ na zakres posiadanych uprawnień do przetwarzania danych osobowych i występowania każdorazowo z wnioskiem o nadanie nowego upoważnienia z uwzględnieniem nowych uprawnień oraz anulowania starego upoważnienia.

11. Administrator bezpieczeństwa informacji jest zobowiązany do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych.

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

1. Użytkownik uzyskuje dostęp do systemu informatycznego, w szczególności do zawierającego dane osobowe, wyłącznie poprzez podanie własnego identyfikatora (loginu) i hasła.
2. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik jest odpowiedzialny za wszystkie czynności wykonane przy użyciu jego identyfikatora.
3. Identyfikator składa się z dowolnej liczby znaków, musi być jednak unikatowy w danym systemie i jednoznacznie identyfikować w nim użytkownika.
4. Użytkownik otrzymuje hasło początkowe z chwilą przystąpienia do pracy w systemie informatycznym i jest zobowiązany zmienić je natychmiast po rozpoczęciu pracy, na sobie tylko znany ciąg znaków.
5. Hasło składa się z co najmniej 8 znaków.
6. Hasło musi zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
7. Hasło nie powinno się składać z kombinacji znaków mogących ułatwić jego odgadnięcie lub odszyfrowanie przez osoby nieuprawnione (np.: imię, nazwisko użytkownika).
8. System informatyczny powinien być wyposażony w mechanizmy wymuszające zmianę hasła nie rzadziej, niż co 30 dni. Jeśli system nie daje takiej możliwości, zmianę hasła po upływie 30 dni zobowiązany jest wymusić na użytkownikach administrator systemu. Jeżeli dane osobowe przetwarzane są poza systemem informatycznym (sieciowym), jednostanowiskowo, za zmianę hasła odpowiada użytkownik
9. Hasło nie może być zapisane w miejscu dostępnym dla osób nieuprawnionych i należy je zachować w tajemnicy, również po upływie ważności.

10. Użytkownik nie może udostępniać osobom nieuprawnionym (w tym również innym pracownikom upoważnionym do przetwarzania danych osobowych w danym systemie, z wyłączeniem w szczególnych przypadkach administratorów systemu lub bazy) swojego identyfikatora oraz hasła.
11. W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest niezwłocznie zmienić hasło oraz powiadomić o tym fakcie administratora systemu (a ten administratora bezpieczeństwa informacji) lub bezpośrednio administratora bezpieczeństwa informacji.
12. Osoby uprawnione do wykonywania prac administracyjnych w systemie informatycznym (zwykle administratorzy systemu lub bazy) posiadają własne konta administracyjne oraz hasła.
13. Komputery pracujące poza systemami sieciowymi (w tym komputery przenośne), w szczególności zawierające dane osobowe muszą być zabezpieczone przed nieuprawnionym dostępem poprzez ustanowienie hasła w BIOS oraz w systemie (np. Windows).
14. Znajdujące się na komputerach przenośnych oraz na zewnętrznych nośnikach (dyskach, dyskietkach, pamięciach flash, płytach CD, DVD, taśmach magnetycznych, kartach pamięci itp.) zbiory zawierające dane osobowe muszą być zabezpieczone poprzez ich zaszyfrowanie uniemożliwiające odczyt osobom nieuprawnionym.

Rozdział 4
Rozpoczęcie, zawieszenie i zakończenie pracy przez użytkowników systemu informatycznego

1. Użytkownik rozpoczynając pracę w systemie informatycznym loguje się do niego podając swój identyfikator oraz hasło dostępu do systemu.
2. Dostęp do danych osobowych możliwy jest jedynie po dokonaniu uwierzytelnienia użytkownika.
3. Maksymalna liczba prób wprowadzenia hasła przy logowaniu się do systemu informatycznego wynosi 3. Po przekroczeniu tej liczby prób logowania system powinien zablokować danemu użytkownikowi (posługującemu się danym identyfikatorem) dostęp do zbioru danych.
4. Komputer pracujący w systemie informatycznym i/lub wykorzystywany do przetwarzania danych osobowych musi być wyposażony w wygaszasz ekranu

zabezpieczony hasłem. W przypadku braku aktywności użytkownika na komputerze przez okres dłuższy, niż 10 minut musi nastąpić automatyczne włączenie wygaszacza ekranu.

5. Monitory stanowisk komputerowych, na których przetwarzane są dane osobowe, znajdujące się w pomieszczeniach, w których mogą przebywać osoby nieupoważnione do przetwarzania danych osobowych, należy ustawić w taki sposób, aby uniemożliwić tym osobom wgląd w dane.
6. Przebywanie osób nieuprawnionych w pomieszczeniach, w których przetwarzane są dane osobowe, jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych.
7. Pomieszczenia, w których przetwarzane są dane osobowe, należy zamykać na czas nieobecności osób upoważnionych, w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.
8. Przed czasowym opuszczeniem stanowiska pracy użytkownik zobowiązany jest:
   1) wylogować się z sytemu informatycznego lub
   2) wywołać blokowany hasłem wygaszasz ekranu.
9. Kończąc pracę użytkownik zobowiązany jest:
   1) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,
   2) zabezpieczyć stanowisko pracy, w tym przede wszystkim złożyć w szafie lub szufladzie biurka zamykanych na klucz wszelką dokumentację związaną z danymi osobowymi oraz nośniki magnetyczne, optyczne i inne, na których znajdują się dane osobowe.

Rozdział 5

Zabezpieczenia systemów informatycznych, tworzenie kopii zapasowych zbiorów danych osobowych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Serwery systemów informatycznych, w których przetwarzane są dane osobowe oraz serwery przechowujące te dane muszą być zabezpieczone odpowiednimi urządzeniami (zasilaczami awaryjnymi - UPS) przed nieprzewidzianymi awariami zasilania.
2. W miarę możliwości również jednostki komputerowe, na których przetwarzane są dane osobowe powinny być zabezpieczone przy pomocy zasilaczy awaryjnych (UPS).

3. Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych.
4. Za tworzenie kopii zapasowych zbiorów danych osobowych przetwarzanych w systemach informatycznych odpowiedzialny jest administrator systemu lub inna osoba przez niego wyznaczona.
5. W przypadku przetwarzania danych osobowych poza systemem informatycznym (sieciowym), jednostanowiskowo, za tworzenie kopii zbiorów danych osobowych przetwarzanych na tym stanowisku odpowiedzialny jest użytkownik.
6. Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu informatycznego. Za przeprowadzanie tej procedury w przypadku systemu informatycznego odpowiedzialny jest jego administrator, a w przypadku danych pochodzących z systemów pozasieciowych, ich użytkownicy.
7. Kopie zapasowe wykonywane są zgodnie z następującym harmonogramem:
   1) kopia zapasowa aplikacji przetwarzającej dane osobowe – pełna kopia wykonywana jest przed i po wprowadzeniu zmian do aplikacji (na przykład instalacji uaktualnień, nowych wersji itp.), nierzadziej jednak, niż raz na 3 miesiące.
   2) kopia zapasowa danych osobowych przetwarzanych przez aplikację – pełna kopia wykonywana jest co najmniej raz w tygodniu, a w przypadku wprowadzenia znacznych zmian danych osobowych po dniu roboczym, w którym dokonano zmian.
   3) kopia zapasowa danych konfiguracyjnych systemu informatycznego przetwarzającego dane osobowe, w tym uprawnień użytkowników systemu –kopia wykonywana jest po każdym dniu roboczym, w którym dokonano modyfikacji uprawnień (w tym dopisania nowych użytkowników).

Rozdział 6

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

1. Użytkownicy nie mogą wynosić poza obiekty Uniwersytetu urządzeń (w tym również komputerów przenośnych) oraz nośników danych zawierających dane osobowe bez zgody przełożonego odpowiedzialnego za przetwarzanie danych osobowych lub administratora bezpieczeństwa informacji.

2. Okresowe kopie zapasowe wykonywane są na dyskietkach, płytach CD, DVD, taśmach lub innych nośnikach danych. Kopie przechowuje się w innych pomieszczeniach i o ile to możliwe w innych budynkach, niż te, w których przechowywane są zbiory danych wykorzystywane na bieżąco. Kopie zapasowe przechowuje się w sposób uniemożliwiający nieuprawnione przejęcie, modyfikacje, uszkodzenie lub zniszczenie.
3. Kopie zapasowe przechowywane są w szafie lub szufladzie zamykanej na klucz.
4. Dostęp do nośników danych z kopiami zapasowymi danych osobowych przetwarzanych w systemach informatycznych (sieciowych) mają wyłącznie administrator systemu (lub osoba wyznaczona przez niego do wykonywania kopii zapasowych) oraz administrator bezpieczeństwa informacji.
5. Dostęp do nośników danych z kopiami zapasowymi danych osobowych przetwarzanych poza systemami informatycznymi (sieciowych), jednostanowiskowo, mają wyłącznie administrator bezpieczeństwa informacji oraz użytkownik wykonujący kopię.
6. Usunięcie danych z systemu powinno zostać zrealizowane przy pomocy oprogramowania przeznaczonego do bezpiecznego usuwania danych z nośnika danych w sposób trwały i uniemożliwiający odczyt.
7. Za zniszczenie kopii zapasowych sporządzanych indywidualnie (lokalnie) przez użytkownika odpowiada użytkownik.
8. Dane osobowe w postaci elektronicznej należy usuwać z nośnika danych w sposób uniemożliwiający ich ponowne odtworzenie, nie później, niż po upływie 5 dni po wykorzystaniu tych danych, chyba że z odrębnych przepisów wynika obowiązek ich dłuższego przechowywania.
9. Nośniki danych, zawierające dane osobowe lub informacje służbowe, przeznaczone do likwidacji pozbawia się wcześniej zapisu tych danych i informacji, a w przypadku, gdy nie jest to możliwe, uszkadza się je w sposób uniemożliwiający ich odczytanie.
10. Likwidację takich nośników nadzoruje uczelniana komisja likwidacyjna, w skład której wchodzi w takim przypadku pracownik właściwego działu odpowiedzialnego za informatyzację Uczelni.
11. Przez zniszczenie nośników danych należy rozumieć ich trwałe i nieodwracalne zniszczenie fizyczne do stanu uniemożliwiającego ich rekonstrukcję i odzyskanie danych i informacji.

12. Nośniki danych zawierające dane osobowe lub informacje służbowe, przeznaczone do przekazania podmiotowi nieuprawnionemu do przetwarzania danych osobowych lub posiadania informacji służbowych Uczelni pozbawia się wcześniej zapisu tych danych i informacji w sposób uniemożliwiający ich odzyskanie.
13. Nośniki danych zawierające dane osobowe lub informacje służbowe, przeznaczone do naprawy pozbawia się wcześniej zapisu tych danych i informacji w sposób uniemożliwiający ich odzyskanie albo naprawia pod nadzorem osoby do tego upoważnionej przez administratora bezpieczeństwa informacji lub administratora systemu informatycznego.

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

1. Za ochronę antywirusową systemu informatycznego (przed wirusami komputerowymi, końmi trojańskimi, robakami komputerowymi, oprogramowaniem szpiegującym, kradnącym dane lub hasła dostępu itp.) odpowiada administrator systemu.
2. System antywirusowy zainstalowany jest w każdym komputerze z dostępem do danych osobowych oraz w każdym komputerze z dostępem do sieci publicznej.
3. Programy antywirusowe są uaktywnione przez cały czas pracy każdego komputera z dostępem do danych osobowych lub z dostępem do sieci publicznej.
4. Wszystkie pliki otrzymywane spoza sieci lokalnej, jak również wysyłane na zewnątrz sieci lokalnej, podlegają automatycznemu sprawdzeniu przez system antywirusowy z zastosowaniem najnowszej dostępnej wersji programu antywirusowego (lub bazy wirusów).
5. W przypadku pojawienia się wirusa, użytkownik zobowiązany jest do zaprzestania wykonywania jakichkolwiek czynności w systemie związanych z przetwarzaniem danych i niezwłocznego powiadomienia administratora systemu lub administratora bezpieczeństwa informacji.
6. Niedozwolone jest otwieranie wiadomości poczty elektronicznej i załączników od „niezaufanych” nadawców.

7. Niedozwolone jest wyłączanie, blokowanie i odinstalowywanie programów zabezpieczających komputer przed złośliwym oprogramowaniem oraz nieautoryzowanym dostępem z zewnątrz (skaner, program antywirusowy, firewall).
8. Administrator systemu odpowiedzialny jest za aktywowanie i poprawne konfigurowanie oprogramowania monitorującego wymianę danych na styku:
   1) sieci lokalnej i publicznej,
   2) stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci lokalnej.

Rozdział 8
Wykonywanie przeglądów i konserwacji systemów oraz nośników danych służących do przetwarzania danych

1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe wykonywane są wyłącznie przez pracowników Działu Informatyzacji.
2. Administrator systemu okresowo sprawdza możliwość odtworzenia danych z kopii zapasowej. Częstotliwość wykonywania procedury odtwarzania danych jest uzgadniana z administratorem bezpieczeństwa informacji.
3. Aktualizacja oprogramowania powinna być przeprowadzana zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji.
4. Za terminowość przeprowadzania przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada administrator systemu.
5. Nieprawidłowości w działaniu systemu informatycznego oraz oprogramowania są usuwane przez pracowników właściwego działu odpowiedzialnego za informatyzację Uczelni, a ich przyczyny analizowane w celu uniknięcia podobnych zdarzeń w przyszłości.

Rozdział 9
Postępowanie w przypadku naruszenia ochrony danych osobowych

1. Każdy pracownik (w szczególności osoba zatrudniona przy przetwarzaniu danych osobowych w systemie informatycznym), który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych przetwarzanych

w Uniwersytecie zobowiązany jest do niezwłocznego poinformowania o tym swojego przełożonego, a ten do poinformowania administratora systemu informatycznego, jeśli zdarzenie dotyczy systemu informatycznego oraz Administratora Bezpieczeństwa Informacji Uniwersytetu.

3. Administrator systemu informatycznego, który stwierdził lub uzyskał informację wskazującą na naruszenie w systemie ochrony danych osobowych zobowiązany jest do niezwłocznego:

   5) zapisania wszelkich informacji i okoliczności związanych z danym zdarzeniem, a w szczególności dokładnego czasu uzyskania informacji o naruszeniu ochrony danych osobowych lub samodzielnym wykryciu tego faktu,

   6) jeżeli zasoby systemu na to pozwalają, wygenerowania i wydrukowania wszystkich dokumentów i raportów, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzenia ich datą i podpisania,

   7) przystąpienia do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym do określenia skali zniszczeń, metody dostępu osoby niepowołanej do danych itp.,

   8) podjęcia odpowiednich kroków w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych, w tym między innymi:

      d) fizycznego odłączenia urządzeń i segmentów sieci które mogły umożliwić dostęp do bazy danych osobie niepowołanej,

      e) wylogowania użytkownika podejrzanego o naruszenie ochrony danych,

      f) zmianę hasła użytkownika, poprzez którego uzyskano nielegalny dostęp w celu uniknięcia ponownej próby uzyskania takiego dostępu,

   7) szczegółowej analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych,

   8) przywrócenia normalnego działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, odtworzenia jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności mających na celu

uniknięcie ponownego uzyskania dostępu przez osobę nieupoważnioną w ten sam sposób.

10. Po przywróceniu normalnego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia, oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

11. Jeżeli przyczyną zdarzenia był błąd użytkownika systemu informatycznego, należy przeprowadzić ponowne szkolenie w zakresie ochrony danych osobowych w systemie informatycznym.

12. Jeżeli przyczyną zdarzenia była infekcja wirusem, należy ustalić źródło jego pochodzenia i wykonać zabezpieczenia antywirusowe i organizacyjne wykluczające powtórzenie się podobnego zdarzenia w przyszłości.

Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Uniwersytecie Kazimierza Wielkiego wchodzi w życie z dniem 01.05.2013 roku.