Zarządzenie nr 6
Rektora Uniwersytetu w Białymstoku
z dnia 16.02.2004 r.

w sprawie ochrony danych osobowych w systemach informatycznych Uniwersytetu w Białymstoku

Na podstawie art. 49 ust. 2 ustawy z dnia 12 września 1990 r. o szkolnictwie wyższym (Dz. U. nr 56 poz. 385 z późniejszymi zmianami) w związku z art. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. nr 101 poz. 926 z 2002 r. z późniejszymi zmianami) oraz § 6 i § 11 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. nr 80 poz. 521 z późniejszymi zmianami) zarządza się, co następuje :

§ 1

Obowiązki administratora danych w Uniwersytecie w Białymstoku wykonuje Rektor przy pomocy :

- Prorektorów – w zakresie wynikającym z powierzonych im zadań,
- Dziekanów, Kierowników jednostek organizacyjnych Uniwersytetu – w zakresie przetwarzanych w ramach jednostki danych osobowych pracowników i studentów,
- Dyrektora Biblioteki Uniwersyteckiej – w zakresie przetwarzanych w bibliotece danych osobowych czytelników,
- Kwestora, Kierownika Działu Spraw Osobowych – w zakresie danych osobowych przetwarzanych przez podległe im jednostki organizacyjne administracji,

zwanych dalej lokalnymi administratorami danych osobowych.

§ 2

Za bezpieczeństwo danych osobowych w systemach informatycznych Uniwersytetu w Białymstoku odpowiada powołany przez Rektora – Administrator bezpieczeństwa informacji.

§ 3

Każda baza danych osobowych w Uniwersytecie tworzona jest za zgodą Rektora i rejestrowana przez Administratora bezpieczeństwa informacji.

§ 4

1. Zasady zarządzania systemem informatycznym służącym do przetwarzania danych określa Instrukcja stanowiąca Załącznik nr 1 do niniejszego Zarządzenia.
2. Zasady postępowania w sytuacji naruszenia ochrony danych osobowych określa Instrukcja stanowiąca Załącznik nr 2 do niniejszego Zarządzenia.

§ 5

Zobowiązuję lokalnych administratorów danych osobowych do przekazania Administratorowi bezpieczeństwa informacji, w terminie 30 dni od wejścia w życie niniejszego Zarządzenia, wniosków o zarejestrowanie baz danych osobowych w systemach informatycznych z uwzględnieniem następujących informacji :

- zakres przetwarzania danych osobowych w bazie,
- obszar (pomieszczenie), w którym dane są przetwarzane,
- dane administratora systemu informatycznego,
- lista pracowników zatrudnionych przy przetwarzaniu danych, z określeniem zakresu uprawnień i identyfikatorów,
- zabezpieczenia techniczne i organizacyjne bazy.

§ 6

Zarządzenie wchodzi w życie z dniem podpisania.

REKTOR
UNIWERSYTETU w BIAŁYMSTOKU
prof. dr hab. Marek Gębczyński

Załącznik nr 1
do Zarządzenia nr 6
Rektora Uniwersytetu w Białymstoku
z dnia 16.02.2004 r.

Instrukcja
w sprawie sposobu zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Uniwersytecie w Białymstoku

§ 1

Do zadań Administratora bezpieczeństwa informacji należy w szczególności:
- określenie strategii zabezpieczania systemów informatycznych Uczelni,
- analiza zagrożeń bezpieczeństwa danych osobowych,
- nadzór nad prawidłowym funkcjonowaniem wszystkich baz danych w Uniwersytecie,
- nadzór nad bezpieczeństwem funkcjonowania wszystkich urządzeń pracujących w systemie,
- nadzór nad właściwym zabezpieczeniem obszaru (pomieszczeń, budynków), w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego,
- nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemach informatycznych,
- prowadzenie ewidencji: baz danych osobowych w systemach informatycznych, osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych, obszarów w których przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego.

§ 2

Lokalni administratorzy danych osobowych:
- wnioskują o zarejestrowanie bazy danych do Rektora,
- stwarzają właściwe warunki techniczno–organizacyjne gwarantujące bezpieczeństwo systemów informatycznych w podległych im jednostkach,
- wyznaczają administratora systemu informatycznego przetwarzającego dane osobowe,
- określają indywidualne zakresy czynności osób zatrudnionych przy przetwarzaniu danych w bazie, a w szczególności zakres uprawnień i odpowiedzialności,
- niezwłocznie przekazują Administratorowi bezpieczeństwa informacji dane o osobach zatrudnionych przy przetwarzaniu danych, ich zakresach czynności (uprawnień), dacie zarejestrowania (bądź wyrejestrowania) w systemie, nadanym identyfikatorze,
- zapoznają osoby zatrudnione przy przetwarzaniu danych z przepisami o ochronie danych osobowych i przekazują do Działu Spraw Osobowych oświadczenia tych osób o zapoznaniu się z przepisami,
- niezwłocznie informują Administratora bezpieczeństwa informacji o wszelkich zmianach w zakresie istniejących baz danych, osób zatrudnionych przy przetwarzaniu danych, lokalizacji pomieszczeń, w których są przetwarzane dane oraz o wszelkich zagrożeniach bezpieczeństwa systemów informatycznych,
- wykonują zalecenia Administratora bezpieczeństwa informacji w zakresie ochrony danych osobowych.

§ 3

1. Administrator bezpieczeństwa informacji prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych, zawierającą następujące informacje:
- imię i nazwisko użytkownika,
- identyfikator,
- datę zarejestrowania w systemie,
- zakres przydzielonych uprawnień,
- datę wyrejestrowania z systemu.
2. Identyfikator użytkownika w systemie informatycznym rejestruje administrator systemu informatycznego.
3. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.
4. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych, administrator systemu informatycznego niezwłocznie wyrejestrowuje z systemu informatycznego.
5. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
6. Hasło użytkownika przydziela i zmienia administrator systemu informatycznego.
7. Hasło użytkownika powinno być zmieniane co najmniej raz w miesiącu.

§ 4

1. Przed rozpoczęciem pracy użytkownik ma obowiązek sprawdzić, czy stan urządzenia nie wskazuje na naruszenie lub próbę naruszenia bezpieczeństwa danych osobowych.
2. Uzytkownik kończący pracę lub czasowo opuszczający stanowisko pracy obowiązany jest do wylogowania się z systemu, z zastrzeżeniem ust. 3
3. Użytkownik nie jest zobowiązany do wylogowania się z systemy w przypadku krótkotrwałego opuszczenia stanowiska pracy pod warunkiem, że wygaszacz monitora zabezpieczony jest hasłem.
4. Administrator systemu informatycznego prowadzi bieżące monitorowanie logowania się do systemu.

§ 5

1. Kopie awaryjne tworzy administrator systemu informatycznego w każdym dniu pracy systemu.
2. Kopie awaryjne przechowywane są przez administratora systemu informatycznego, który dokonuje ich okresowego sprawdzania pod kątem dalszej przydatności do odtworzenia danych w przypadku awarii sytemu i usuwa bezzwłocznie po ustaniu ich użyteczności.

§ 6

1. Urządzenia systemu informatycznego, w którym przetwarzane są dane osobowe należy zabezpieczyć systemami antywirusowymi.
2. System informatyczny winien być stale sprawdzany pod kątem obecności wirusów komputerowych.
3. Systemy antywirusowe winny być bieżąco uaktualniane.

§ 7

Nośniki informacji zawierająca dane osobowe, w tym kopie informatyczne i wydruki, przechowywane są w warunkach uniemożliwiających dostęp do nich osobom niepowołanym i usuwane są bezzwłocznie po ustaniu ich użyteczności.

§ 8

Przeglądy i konserwację systemu i zbioru danych przeprowadza administrator systemu informatycznego.

§ 9

Lokalna sieć komputerowa, w której przetwarzane są dane osobowe powinna być zabezpieczona w miejscu połączenia z siecią zewnętrzną co najmniej systemem typu „Fire Wall". W ramach zabezpieczeń połączeń sieci lokalnej z siecią zewnętrzną, powinny zostać zablokowane wszystkie usługi sieciowe, poza niezbędnymi dla działania systemów obsługujących dane osobowe oraz dostępu do podstawowych usług informacyjnych: poczty elektronicznej, WWW itp.

§ 10

1. W przypadku przetwarzania danych osobowych zdalnie poprzez sieć komputerową, dostęp do serwera bazy danych osobowych powinien odbywać się z wykorzystaniem zabezpieczeń kryptograficznych, które uniemożliwiają odczyt danych w momencie autoryzacji i w trakcie transmisji danych.
2. Informacja o wszystkich zdarzeniach związanych z dostępem do serwera bazy danych osobowych powinna być zbierana i przechowywana.

Załącznik nr 2
do Zarządzenia nr 6
Rektora Uniwersytetu w Białymstoku
z dnia 16.02.2004 r.

Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych w systemach informatycznych Uniwersytetu w Białymstoku

§ 1

Niniejsza instrukcja określa tryb postępowania w przypadku:
1) stwierdzenia naruszenia zabezpieczenia danych w systemie informatycznym,
2) wystąpienia zmian sposobu działania systemu które mogą wskazywać na naruszenie zabezpieczenia danych (np. zmiana w sposobie działania urządzeń, zmiana zawartości zbioru danych osobowych, zmiana w sposobie działania programu, nietypowa i niezgodna z dotychczasowym doświadczeniem, zmiana sposobu i jakości komunikacji w sieci telekomunikacyjnej).

§ 2

Każda osoba zatrudniona przy przetwarzaniu danych osobowych, która stwierdzi lub podejrzewa naruszenie ochrony danych osobowych zobowiązana jest:
1) niezwłocznie poinformować o tym Administratora bezpieczeństwa informacji lub upoważnioną przez niego osobę, a w przypadku jego nieobecności Kierownika jednostki,
2) przerwać pracę i nie podejmować dalszych czynności bez zgody Administratora bezpieczeństwa informacji, celem zabezpieczenia stanu systemu w momencie stwierdzenia naruszenia bezpieczeństwa.

§ 3

W przypadku stwierdzenia lub podejrzenia naruszenia zabezpieczeń danych osobowych Administrator bezpieczeństwa informacji powinien podjąć niezwłocznie następujące czynności:

1. Zapisać i zabezpieczyć informacje o stanie systemów i potencjalnym naruszeniu ochrony danych:
   1) zapisać wszelkie informacje związane z danym zdarzeniem, a w szczególności dokładny czas uzyskania informacji o naruszeniu ochrony danych osobowych,
   2) niezwłocznie wygenerować i wydrukować (jeśli zasoby systemu na to pozwalają) wszelkie możliwe dokumenty i raporty systemowe, które mogą pomóc w ustalaniu okoliczności zdarzenia, opatrzyć je data i podpisem,
   3) przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody jaką osoba nieuprawniona uzyskała dostęp do danych osobowych.

2. Podjąć odpowiednie działania w celu powstrzymania lub ograniczenia dostępu do danych przez osoby nieuprawnione, zminimalizowania szkód, zabezpieczenia systemu informatycznego, w szczególności poprzez:
   1) fizyczne odłączenie urządzeń i segmentów sieci, które mogły umożliwić dostęp do danych osobie nieuprawnionej,

2) wylogowanie użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych,
3) zmianę haseł administratora i użytkownika (przez które uzyskano nieuprawniony dostęp do danych osobowych) w celu uniemożliwienia ponownego uzyskania nieuprawnionego dostępu do danych.

3. Po wyeliminowaniu bezpośredniego zagrożenia Administrator bezpieczeństwa informacji powinien przeprowadzić wstępną analizę stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych. W tym celu powinien sprawdzić w szczególności:
1) stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
2) zawartość zbioru danych osobowych,
3) sposób działania programu używanego do przetwarzania danych osobowych,
4) jakość komunikacji w sieci teleinformatycznej, w tym fakt nieuprawnionego zdalnego dostępu do systemów związanych z przetwarzaniem danych osobowych, złamanie zabezpieczeń systemów,
5) możliwość obecności wirusów komputerowych.

§ 4

Po stwierdzeniu naruszenia ochrony danych osobowych Administrator bezpieczeństwa informacji powinien:
1) przeprowadzić szczegółową analizę stanu systemu informatycznego i określić okoliczności i przyczyny, które doprowadziły do naruszenia bezpieczeństwa danych,
2) przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości,
3) przygotować szczegółowy raport o skutkach, przyczynach, przebiegu i wnioskach ze zdarzenia i przekazać je Rektorowi i Kierownikowi jednostki organizacyjnej.