Załącznik nr 2 do
zarządzenia nr 30/2008

Instrukcja zarządzania systemami informatycznymi używanymi do przetwarzania danych osobowych w Uniwersytecie Przyrodniczym we Wrocławiu

§ 1

Niniejsza instrukcja określa ogólne zasady zarządzania każdym systemem informatycznym służącym do przetwarzania danych osobowych, realizację zadań bezpieczeństwa zbiorów danych przetwarzanych w Uczelni oraz stanowi podstawę do opracowania instrukcji szczegółowych uwzględniających specyfikę poszczególnych systemów informatycznych funkcjonujących na Uczelni.

§ 2

1. ABI Uczelni realizuje następujące zadania:
   a) sprawuje nadzór nad wdrażaniem niniejszej instrukcji we wszystkich systemach informatycznych Uczelni, w których przetwarzane są dane osobowe oraz dba o bieżące jej przystosowanie do zmieniających się technologii informatycznych oraz zagrożeń bezpieczeństwa systemów informatycznych,
   b) wytycza strategię zabezpieczania systemów informatycznych Uczelni,
   c) identyfikuje i aktualizuje zagrożenia oraz ryzyko, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych Uczelni,
   d) określa potrzeby w zakresie zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe,
   e) monitoruje działanie zabezpieczeń wdrożonych w celu ochrony danych osobowych w systemach informatycznych oraz ich przetwarzania.

§ 3

1. Głównym zadaniem lokalnych administratorów jest przeciwdziałanie dostępowi osób niepowołanych do systemów informatycznych, w którym przetwarzane są dane osobowe poprzez zapewnienie właściwych warunków organizacyjno-technicznych gwarantujących bezpieczeństwo systemów informatycznych w podległych im jednostkach organizacyjnych Uczelni oraz podejmowanie odpowiednich działań w przypadku wykrycia takich naruszeń w systemach.
2. Do szczególnych zadań lokalnych administratorów należy:
   1) wyznaczanie administratorów systemów informatycznych funkcjonujących w podległych im jednostkach,
   2) stosowanie się do zaleceń ABI i uwzględnianie w miarę możliwości finansowo-lokalowych zaleceń ABI w zakresie:
      a) wskazania budynków, pomieszczeń lub części pomieszczeń tworzących obszary, w których przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego,
      b) nadzoru nad technicznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe oraz kontrola przebywania w nich osób,
      c) określenia miejsca i sposobu przechowywania kopii awaryjnych zbiorów danych osobowych,
      d) wskazania sposobu zabezpieczeń: krat, systemów monitoringu i awaryjnych adekwatnych do zagrożenia systemów informatycznych,
      e) dokonywania zakupu systemów operacyjnych, oprogramowania antywirusowego oraz systemów kryptograficznych, które podwyższają bezpieczeństwo danych osobowych oraz gwarantują spełnienie wymogów określonych ustawą,

f) dokonywania zakupu pamięci masowych, streamerów oraz innych urządzeń i nośników, które umożliwiają wykonywanie kopii zapasowych danych osobowych w systemach informatycznych,
g) właściwego prowadzenia i zabezpieczenia okablowania sieci komputerowej przeznaczonej do przetwarzania danych osobowych w systemach informatycznych, w celu uniemożliwienia stosowania podsłuchu lub narażenia infrastruktury sieciowej na zniszczenia,
h) dokonywania zakupu niszczarek jako niezbędnego wyposażenia pomieszczeń, w których generowane są wydruki i kopie na nośnikach zawierające dane osobowe lub uzgodnienia innego dopuszczalnego sposobu niszczenia wydruków i nośników zawierających dane osobowe,
i) dokonywania zakupu szaf pancernych do przechowywania kopii zapasowych danych osobowych z systemów informatycznych.

3) w przypadku, gdy systemy informatyczne działają w środowisku sieciowym :
   a) zalecanie stosowania wskazanej technologii, która minimalizuje zagrożenie uzyskania dostępu do sieci osobom nieupoważnionym,
   b) dokonywanie zakupu oprogramowania umożliwiającego wykorzystanie identyfikatorów przez logujących się do sieci,
   c) nadzorowanie procesu monitorowania sieci pod kątem zabezpieczenia przed dostępem osób nieupoważnionych.
4) zapewnienie odpowiedniego zabezpieczenia budynków oraz pomieszczeń, w których przetwarzane są dane osobowe w systemach informatycznych przed dostępem osób niepowołanych, w zakresie:
   a) określenia listy osób upoważnionych do pobierania kluczy i przebywania w pomieszczeniach, w których przetwarzane są dane osobowe wraz z kontrolą ewidencji czasu pobierania i zdawania kluczy,
   b) określenia trybu szkoleń portierów w budynkach, w których przetwarzane są dane osobowe w systemach informatycznych oraz osób sprzątających pomieszczenia, w których przetwarzane są dane osobowe w systemach informatycznych.
5) przygotowania zasad i ewidencji wykonywania czynności serwisowych w systemach informatycznych w podległych jednostkach w celu wyeliminowania:
   a) możliwości wykonania kopii danych osobowych przez osoby nieupoważnione,
   b) przemieszczania urządzeń komputerowych i ich części służących do przetwarzania danych osobowych poza obszar objęty ochroną,
   c) podmiany elementów sprzętu komputerowego lub oprogramowania na inny, który zawiera niepożądane cechy ukryte.

§ 4

1. ASI mają za zadanie opracowanie i bieżące uaktualnianie, z pomocą administratorów poszczególnych systemów informatycznych, szczegółowych instrukcji dotyczących zarządzania systemami informatycznymi w podległych im systemach informatycznych, które powinny zawierać w szczególności:
   1) zasady przydziału haseł dla użytkowników poszczególnych systemów informatycznych i częstotliwość ich zmiany oraz wskazanie osoby odpowiedzialnej za te czynności,
   2) sposób rejestrowania i wyrejestrowywania użytkowników z systemu informatycznego oraz wskazanie osoby odpowiedzialnej za te czynności,
   3) procedury rozpoczęcia i zakończenia pracy,
   4) metody i częstotliwość wykonywania kopii awaryjnych,
   5) metody i częstotliwość sprawdzania systemów informatycznych na obecność wirusów komputerowych oraz metodę ich usuwania,
   6) sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków,

7) sposób postępowania w zakresie komunikacji w sieci komputerowej.

2. ASI są zobowiązani do:
   1) wykonywania poleceń ABI w zakresie zarządzania podległymi systemami informatycznymi,
   2) czuwania nad właściwym eksploatowaniem podległych im systemów informatycznych,
   3) prowadzenia, uaktualniania na bieżąco oraz przesyłania ABI, danych w zakresie:
      a) listy osób uczestniczących w przetwarzaniu danych osobowych,
      b) lokalizacji pomieszczeń, w których te dane są przetwarzane, w przypadku zaistnienia jakichkolwiek zmian tych lokalizacji,
      c) rodzaju systemów informatycznych funkcjonujących w zakresie ich działalności,
      d) listy identyfikatorów osób uczestniczących w przetwarzaniu danych osobowych w podległych im systemach informatycznych,
      e) czynności serwisowych wykonywanych w podległych systemach informatycznych,
      f) zdarzeń wpływających na bezpieczeństwo systemów informatycznych, w tym między innymi:
         – wykrytych wirusów, koni trojańskich itp.,
         – oprogramowania nielegalnego lub zainstalowanego bez upoważnienia,
         – awarii systemu informatycznego lub jego nieprawidłowego działania,
         – stwierdzenia faktu korzystania z systemu informatycznego przez osobę niepowołaną,
         – awarii zasilania,
   4) kontrolowania i zabezpieczania prawidłowego przebiegu czynności serwisowych w podległych systemach informatycznych, przy czym: w przypadku, gdy urządzenia, dyski lub inne nośniki zawierające dane osobowe, przed naprawą obowiązkowo należy usunąć zapis tych danych lub osobiście nadzorować naprawę,
   5) pozbawiania zapisu danych osobowych tych nośników, które przeznaczone są do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania tych danych,
   6) pozbawiania zapisu danych osobowych lub uszkadzania w sposób uniemożliwiający odczytanie tych nośników, które przeznaczone są do likwidacji,
   7) instalowania zabezpieczeń w podległych systemach informatycznych, wynikających z zaleceń ABI,
   8) zgłaszania lokalnym administratorom danych oraz ABI – potrzeb w zakresie zabezpieczenia podległych im systemów informatycznych,
   9) postępowania zgodnie z instrukcją w sytuacji naruszenia zasad ochrony danych osobowych,
   10) okresowego sprawdzania kopii awaryjnych pod kątem prawidłowości ich wykonania oraz ich dalszej przydatności do odtworzenia w przypadku awarii,
   11) znajomości oraz posiadania dokumentacji funkcji poszczególnych systemów informatycznych, ze szczególnym uwzględnieniem procedur:
      a) dostępu do danych osobowych i ich modyfikowania,
      b) zarządzania identyfikatorami,
      c) wykonywania kopii awaryjnych oraz odtwarzania danych z tych kopii,
      d) generowania wydruków danych osobowych,
      e) dostępu do plików rejestrujących identyfikatory oraz czas logowania użytkowników.

§ 5

Administratorzy poszczególnych systemów informatycznych służących do przetwarzania danych osobowych odpowiadają za ich bieżącą eksploatacje, a w szczególności za:

– wszystkie czynności związane z ich funkcjonowaniem i modernizacją,
– rejestrowanie i wyrejestrowywanie z systemu użytkowników, a także serwis w czasie instalowania systemu oraz jego modyfikacji,
– przydzielanie uprawnień do poszczególnych funkcji systemu oraz określenie trybu i częstotliwości zmiany haseł,
– procedury wykonywania kopii awaryjnych, określanie ich częstotliwości, zmianę nośników oraz ich właściwe przechowywanie, sprawdzanie poprawności zapisu i likwidacje,

– lokalizację sprzętu komputerowego, ustawienie monitorów i drukarek uniemożliwiające wgląd w dane osobowe osobom nieupoważnionym lub kradzież wymiennych nośników danych,
– postępowania zgodnie z instrukcją w sytuacji naruszenia ochrony danych osobowych.

§ 6

1. Przy realizacji zasad bezpieczeństwa zbiorów danych osobowych przetwarzanych w Uczelni wprowadza się obowiązek prowadzenia dokumentacji odzwierciedlającej wykonywanie zadań z zakresu ochrony danych osobowych.
2. Dokumentacja, o której mowa w ust. 1, obejmuje:
   a) wykaz informatycznych baz danych, w których przetwarzane są dane osobowe w Uczelni (wzór dokumentu stanowi załącznik nr 4),
   b) ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych i ich identyfikatorów (wzór stanowi załącznik nr 5),
   c) Wykaz miejsc przetwarzania danych osobowych w systemach informatycznych w Uczelni (wzór stanowi załącznik nr 6),
   d) oświadczenia osób przetwarzających dane osobowe (wzór stanowi załącznik nr 7),
   e) wniosek o nadanie/odwołanie upoważnienia do przetwarzania danych osobowych (wzór stanowi załącznik nr 8).
3. Dokumentację, o której mowa w ust. 2, prowadzą osoby uprawnione, zgodnie z instrukcją szczegółową.

§ 7

1. Niniejsza instrukcja przeznaczona jest dla użytkowników i ich przełożonych, którzy nadzorują przetwarzanie danych osobowych i realizację zasad bezpieczeństwa zbiorów baz danych w Uczelni.
2. Wykonanie postanowień niniejszej instrukcji, jak również wydanej na jej podstawie instrukcji szczegółowej ma na celu wprowadzenie jednolitego systemu bezpieczeństwa przetwarzania danych osobowych w Uczelni.

§ 8

1. Zmiany instrukcji oraz instrukcje szczegółowe mogą być wprowadzone zarządzeniem rektora .
2. W sprawach nieuregulowanych niniejszą instrukcją znajdują zastosowanie przepisy ustawy i rozporządzenia.