Zarządzenie Nr 23/OC/2007
Rektora Akademii Rolniczej im. Hugona Kołłątaja w Krakowie
z dnia 28 grudnia 2006 roku

w sprawie: ustalenia zadań Administratora Systemów i Sieci Teleinformatycznej

Na podstawie:
-) art.66 ust. 1 i ust. 2 pkt. 5 Ustawy z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym (Dz. U. z 2005 r. Nr 164 poz. 1365 z późn. zm.),
-) Ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (tekst jednolity Dz. U. z 2005 r. Nr 196 poz. 1631 z późn. zm.),
-) Rozporządzenia Prezesa RM z dnia 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U z 2005 r. Nr 171, poz. 1433),
-) Szczególnych Wymagań Bezpieczeństwa Teleinformatycznego – dopuszczonych uzgodnieniem Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego p. wch. Nr Pf-9/OC-I/2006 zał. 1/40,
-) Procedur Bezpiecznej Eksploatacji Systemu Teleinformatycznego – dopuszczonych uzgodnieniem Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego p. wch. Nr Pf-9/OC-I/2006 zał. 2/38 - do wglądu dla osób uprawnionych do dostępu do informacji stanowiących tajemnicę służbową oznaczonych klauzulą „Zastrzeżone",

zarządza się, co następuje:

§ 1

Z dniem 1 stycznia 2007 r. funkcję i zadania Administratora Systemów i Sieci Teleinformatycznej powierzam Kierownikowi Działu Informatycznego – Głównemu Informatykowi.

§ 2

1. Administrator Systemów i Sieci Teleinformatycznej zwany dalej „Administratorem" podlega Prorektorowi ds. Nauki i Współpracy Międzynarodowej.

2. Administrator jest odpowiedzialny za funkcjonowanie systemu i sieci oraz przestrzeganie zasad i wymagań bezpieczeństwa teleinformatycznego (TI), a w szczególności w zakresie ochrony informacji niejawnych, a także informacji chronionych nie oznaczonych klauzulą tajności, uznanych za ważne dla interesu uczelni, jej pracowników i studentów.

3. Do zakresu obowiązków Administratora należy:
   1) prowadzenie analizy przewidywanych zagrożeń bezpieczeństwa systemu i sieci TI, oraz wytwarzanych, przetwarzanych i przechowywanych w systemie informacji,
   2) opracowanie projektów szczególnych wymagań bezpieczeństwa systemu lub sieci TI oraz propozycji ich uaktualnienia,
   3) instalowanie systemu operacyjnego i przydzielanie uprawnień użytkownikom, zgodnie z poleceniem, i z zakresem określonym przez kierownika jednostki organizacyjnej, a w stosunku do informacji niejawnych - przez pełnomocnika ds. ochrony informacji niejawnych,
   4) szkolenie użytkowników w zakresie zasad i procedur bezpieczeństwa obowiązujących podczas pracy w systemie, w którym przetwarzane będą informacje niejawne i chronione,
   5) okresowa i doraźna obsługa techniczna systemu,

6) nadzorowanie poprawności wykonywania kopii zapasowych danych przez użytkowników,
7) sprawdzanie poprawności działania systemu oraz jego zabezpieczeń,
8) wdrażanie procedur bezpieczeństwa oraz nadzór nad funkcjonowaniem systemu,
9) wdrażanie procedur ochrony antywirusowej,
10) opracowanie planów awaryjnych i planu napraw systemu,
11) informowanie pełnomocnika ochrony informacji niejawnych o stwierdzonych naruszeniach bezpieczeństwa systemu oraz wykrytych wirusach i innych zagrożeniach,
12) proponowanie zmian mających na celu zwiększenie bezpieczeństwa systemów i sieci TI,
13) prowadzenie „Dziennika Administratora Systemu i Sieci TI" przechowywanego przy każdym zestawie komputerowym, w którym przetwarzane są informacje niejawne i chronione.

§ 3

Administrator prowadzi analizę przewidywanych zagrożeń wewnętrznych i zewnętrznych w elektronicznym środowisku bezpieczeństwa, biorąc pod uwagę ochronę informacji niejawnych stanowiących tajemnicę służbową oraz informacji chronionych, w szczególności:

1) zagrożeń wewnętrznych:
   a) możliwość naruszenia integralności danych przetwarzanych w systemie TI poprzez modyfikacje, dodanie lub zniszczenie danych,
   b) niepowołany dostęp do systemu TI, w którym przetwarzane są informacje niejawne i chronione,
   c) fizyczne zniszczenie elementów lub całości infrastruktury technicznej systemu TI,
   d) nieodpowiednie parametry pracy systemu TI (np. temperatura, wilgotność, zamoczenie, itp.);
2) zagrożeń zewnętrznych systemów włączonych do w sieci TI:
   a) działania mające na celu poznanie konfiguracji i rodzaju zabezpieczeń systemu,
   b) podsłuchiwanie sieci TI,
   c) podszywanie się pod innego nadawcę , zmiana nagłówków przesyłanych pakietów, oszukiwanie systemu firewall, przejęcia uwierzytelnionego połączenia do atakowanego systemu TI,
   d) wykorzystywanie błędów w systemie operacyjnym systemu TI,
   e) uniemożliwianie poprawnej pracy systemu przez blokowanie systemu TI lub jego poszczególnych usług,
   f) nieświadome instalowanie (uruchamianie) programów tzw. koni trojańskich,
   g) przyjmowanie informacji z sieci za pośrednictwem pocztowych plików informacji w których świadomie zainstalowane są programy – wirusy.

§ 4

1. Przy opracowaniu szczególnych wymagań bezpieczeństwa systemów i sieci TI, Administrator zobowiązany jest uwzględnić:
   1) charakterystykę systemu lub sieci,
   2) dane o budowie systemu lub sieci,
   3) środki ochrony zapewniające bezpieczeństwo informacji niejawnych i chronionych, przetwarzanych w systemie lub sieci, przed możliwością narażenia ich bezpieczeństwa, a w szczególności nieuprawnionym ujawnieniem.

2. Charakterystyka systemu lub sieci powinna określać:
   1) klauzulę tajności informacji niejawnych lub rodzaj informacji chronionych, które będą wytwarzane, przetwarzane lub przechowywane w systemie,
   2) kategorie uprawnień użytkowników systemu lub sieci w zakresie dostępu do wytwarzanych w nich informacji niejawnych,

3. W danych o budowie systemu lub sieci TI należy przedstawić informacje z zakresu:
   1) lokalizacji systemu,
   2) architektury systemu TI (sprzęt i jego konfiguracja, oprogramowanie systemowe, użytkowe i antywirusowe),
   3) opisu środowiska bezpieczeństwa (globalnego, lokalnego i elektronicznego).

§ 5

1. Administrator odpowiedzialny jest za instalowanie systemu operacyjnego w zestawie komputerowym, w którym przetwarzane będą informacje niejawne i chronione.

2. Administrator podejmuje decyzję o zainstalowaniu programu lub aplikacji w systemie i naprawie bądź wymianie zespołu, części lub dysku twardego, na wniosek użytkownika systemu, po uprzednim sprawdzeniu jego właściwości użytkowych.

3. Administrator podejmuje również decyzję o włączeniu systemu po naprawie i stwierdzeniu właściwego jego skonfigurowania.

§ 6

1. Administrator dokonuje okresowego - lub doraźnego, na wniosek użytkownika, sprawdzenia poprawności działania systemu oraz jego zabezpieczeń.

2. Administrator posiada wyłączne prawo zmiany oprogramowania lub jego uaktualnienia w systemie TI, w którym będą przetwarzane informacje niejawne i chronione.

3. Czynności wprowadzenia do użytku nowego oprogramowania lub jego uaktualnienia oraz przeprowadzenie przeglądu systemu i jego zabezpieczeń, Administrator odnotowuje w „Dzienniku Administratora Systemu i Sieci TI".

§ 7

1. Administrator jest odpowiedzialny za nadzór nad czynnościami użytkowników systemu TI, opisanymi w „Procedurach Bezpiecznej Eksploatacji Systemu TI", w których przetwarzane są informacje niejawne i chronione.

2. Administrator nadzoruje czynności:
   1) przywracania systemu operacyjnego i tworzenia kopii zapasowych w trybie awaryjnym,
   2) postępowania w przypadku wystąpienia błędów w funkcjonowaniu systemu lub wykrycia wirusa komputerowego,
   3) postępowania w warunkach zagrożeń środowiskowych i akcjach sabotażu i terroru.

3. Administrator informuje Pełnomocnika ds. ochrony informacji niejawnych, o stwierdzonych naruszeniach bezpieczeństwa systemu TI oraz wykrytych wirusach i innych zagrożeniach wymienionych w § 3 niniejszego zarządzenia.

§ 8

1. Administrator w zakresie wdrażania procedur ochrony antywirusowej ma obowiązek ustawić czynności programu antywirusowego w systemach TI , w których przetwarzane są informacje niejawne i chronione tak, aby program skanował dyski i foldery oraz rejestrował zdarzenia i monitorował system operacyjny.

2. Czynności, o których mowa wyżej, Administrator wykonuje w uzgodnieniu z użytkownikiem systemu TI, uwzględniając potrzeby i wymogi związane z ustawowym obowiązkiem ochrony informacji niejawnych i chronionych.

3. Administrator przegląda i sprawdza szczegółowe informacje zapisane w dzienniku zdarzeń programu antywirusowego, raz na miesiąc (30 dni) w szczególności związanych z bezpieczeństwem systemu, przede wszystkim:
   1) informacje o monitorowaniu błędów,
   2) monitorowania zdarzeń dotyczących określonych zbiorów,
   3) skanowania systemu,
   4) wykrywania niepokojących zachowań lub zagrożeń.

§ 9

Czynności opisane w § 9, Administrator ewidencjonuje w „Dzienniku Administratora Systemu i Sieci TI".

§ 10

Administrator, w celu zwiększenia bezpieczeństwa systemów i sieci oraz ochrony przetwarzanych informacji niejawnych i chronionych przedstawia wnioski i propozycje rozwiązań w zakresie zarządzania bezpieczeństwem TI, Prorektorowi ds. Nauki i Współpracy Międzynarodowej wraz z opinią Pełnomocnika ds. ochrony informacji niejawnych.

§ 11

Traci moc obowiązującą Zarządzenie Nr 15/OC/99 Rektora Akademii Rolniczej im. Hugona Kołłątaja w Krakowie z dnia 7 maja 1999 r. w sprawie powołania Administratora Systemu i Sieci Teleinformatycznych, w części dotyczącej powierzenia funkcji i ustalenia zadań.

§ 12

Zarządzenie wchodzi w życie z dniem 1 stycznia 2007 roku.

Kraków, dnia 28 grudnia 2006 r.

Rektor

prof. dr hab. Janusz Żmija

JM/WD/HK

10.01.2007 r.