Załącznik nr 1 do Zarządzenia nr 10/2010

Rektora Akademii Sztuk Pięknych w Warszawie

z dnia 02 marca 2010 r.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w ASP w Warszawie.

1. Niniejsza instrukcja określa ogólne zasady zarządzania każdym systemem informatycznym służącym do przetwarzania danych osobowych w Akademii Sztuk Pięknych w Warszawie, oraz stanowi podstawę do opracowania instrukcji szczegółowych uwzględniających specyfikę poszczególnych systemów informatycznych funkcjonujących na uczelni.

2. Administrator bezpieczeństwa informacji ASP

a) Czuwa nad wdrażaniem niniejszej instrukcji w systemach informatycznych Akademii Sztuk Pięknych w Warszawie, w których przetwarzane są dane osobowe oraz dba o bieżące jej uaktualnianie stosownie do zmieniających się technologii informatycznych oraz zagrożeń bezpieczeństwa systemów informatycznych uczelni.
b) Określa strategię zabezpieczania systemów informatycznych uczelni.
c) Identyfikuje i analizuje zagrożenia oraz ryzyko, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych uczelni.
d) Określa lub zgłasza 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.
f) Wyznacza administratorów bezpieczeństwa informacji obiektów.

3. Lokalni administratorzy danych osobowych stwarzają właściwe warunki organizacyjno-techniczne gwarantujące bezpieczeństwo systemów informatycznych w podległych im jednostkach, a w szczególności:

a) Wyznaczają administratorów poszczególnych systemów informatycznych funkcjonujących w podległych im jednostkach.

b) Stosują się do zaleceń administratora bezpieczeństwa informacji (uwzględniają w miarę możliwości finansowo-lokalowe zalecenia administratora bezpieczeństwa informacji) w zakresie:

- lokalizacji pomieszczeń, w których przetwarzane są dane osobowe
- lokalizacji pomieszczeń, w których przechowywane są kopie awaryjne zbiorów danych osobowych
- instalowania systemów dostępowych i systemów alarmowych adekwatnych do zagrożenia systemów informatycznych
- zakupu systemów operacyjnych, baz danych, oprogramowania antywirusowego oraz systemów

- kryptograficznych podnoszących bezpieczeństwo danych osobowych oraz gwarantujących spełnienie wymogów określonych ustawą
- zakupu pamięci masowych, streamerów oraz innych urządzeń i nośników umożliwiających wykonywanie kopii zapasowych danych osobowych w systemach informatycznych
- właściwego prowadzenia i zabezpieczenia okablowania sieci komputerowej służącej do przetwarzania danych osobowych w systemach informatycznych w celu wyeliminowania niebezpieczeństwa podsłuchu lub zniszczenia infrastruktury sieciowej
- zakupu niszczarek do dokumentów do pomieszczeń, w których generowane są wydruki zawierające dane osobowe
- zakupu szaf pancernych do przechowywania kopii zapasowych danych osobowych z systemów informatycznych

c) Współpracują z administratorami bezpieczeństwa informacji obiektów.

d) W przypadku systemów informatycznych działających w środowisku sieciowym:
- dokonują wyboru lub migracji do technologii minimalizującej zagrożenie uzyskania dostępu do sieci
- osobom nieupoważnionym,
- zakupują oprogramowanie umożliwiające rejestrowanie uaktywniania i czas logowania użytkowników sieci,
- nadzorują proces monitorowania sieci pod kątem zabezpieczenia przed dostępem osób nieupoważnionych.

e) Zabezpieczają budynki oraz pomieszczenia, w których przetwarzane są dane osobowe w systemach informatycznych przed dostępem osób niepowołanych, a w szczególności:
- wprowadzają i nadzorują bieżącą aktualizację listy osób upoważnionych do pobierania kluczy do pomieszczeń, w których przetwarzane są dane osobowe,
- wprowadzają ewidencję osób pobierających klucz do pomieszczeń, w których przetwarzane są dane osobowe zawierającą m.in. czas pobierania i zdawania kluczy,
- określają tryb szkolenia portierów w budynkach, w których przetwarzane są dane osobowe w systemach informatycznych,
- określają tryb szkolenia osób sprzątających pomieszczenia, w których przetwarzane są dane osobowe w systemach informatycznych uwzględniający specyfikę konserwacji systemów komputerowych.

f) Określają zasady i ewidencję wykonywania czynności serwisowych w systemach informatycznych w podległych jednostkach w celu wyeliminowania:
- możliwości wykonania kopii danych osobowych przez osoby nieupoważnione,
- przemieszczania urządzeń komputerowych i ich części służących do przetwarzania danych osobowych poza obszar objęty ochroną,
- podmiany elementów sprzętu komputerowego lub oprogramowania na inny, który zawiera cechy ukryte.

4. Obiektowi i wydziałowi administratorzy sieci komputerowej opracowują i na bieżąco uaktualniają, z pomocą administratorów poszczególnych systemów informatycznych, załączniki do instrukcji zarządzania systemami informatycznymi, które powinny zawierać w szczególności:

a) Sposób przydziału haseł dla użytkowników poszczególnych systemów informatycznych i częstotliwość ich zmiany oraz wskazanie osoby odpowiedzialnej za te czynności.
b) Określenie sposobu rejestrowania i wyrejestrowywania użytkowników oraz wskazanie osoby odpowiedzialnej za te czynności.
c) Procedury rozpoczęcia i zakończenia pracy.
d) Metody i częstotliwość wykonywania kopii awaryjnych.
e) Metody i częstotliwość sprawdzania systemów informatycznych na obecność wirusów komputerowych oraz metodę ich usuwania.
f) Sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków.
g) Sposób postępowania w zakresie komunikacji w sieci komputerowej.

5. Obiektowi i wydziałowi administratorzy sieci komputerowej są zobowiązani do:

a) Wykonywania poleceń administratora bezpieczeństwa informacji ASP w zakresie zarządzania podległymi systemami informatycznymi.
b) Czuwania nad właściwym eksploatowaniem podległych im systemów informatycznych.
c) Prowadzenia, uaktualniania na bieżąco oraz przesyłania administratorowi bezpieczeństwa informacji danych ASP w zakresie:

- listy osób biorących udział przy przetwarzaniu danych osobowych,
- lokalizacji pomieszczeń, w których te dane są przetwarzane, w przypadku zaistnienia jakichkolwiek zmian tych danych,
- rodzaju systemów informatycznych funkcjonujących w zakresie ich działania,
- listy identyfikatorów osób biorących udział przy przetwarzaniu danych osobowych w podległych im systemach informatycznych,
- czynności serwisowych wykonywanych w podległych systemach informatycznych,
- zdarzeń wpływających na bezpieczeństwo systemów informatycznych, w tym m.in.
  -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

d) Kontrolowania i zabezpieczenia prawidłowości przebiegu czynności serwisowych w podległych systemach informatycznych, przy czym urządzenia, dyski lub inne nośniki zawierające dane osobowe, pozbawiają przed naprawą zapisu tych danych lub nadzorują ich naprawę.
e) Pozbawiania zapisu danych osobowych z tych nośników, które przeznaczone są do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania tych danych.
f) Pozbawiania zapisu danych osobowych lub uszkadzania w sposób uniemożliwiający odczytanie tych nośników, które przeznaczone są do likwidacji.
g) Instalowania zabezpieczeń w podległych systemach informatycznych wynikających z zaleceń administratora bezpieczeństwa informacji ASP.

h) Zgłaszania wydziałowym administratorom danych oraz administratorowi bezpieczeństwa informacji ASP potrzeb w zakresie zabezpieczenia podległych im systemów informatycznych.
i) Postępowania zgodnie z instrukcją w sytuacji naruszenia ochrony danych osobowych.
j) Kontrolowania procesu okresowego sprawdzania przez administratorów poszczególnych systemów informatycznych kopii awaryjnych pod kątem prawidłowości ich wykonania oraz ich dalszej przydatności do odtworzenia w przypadku awarii.
k) Znajomości oraz posiadania dokumentacji funkcji poszczególnych systemów informatycznych ze szczególnym uwzględnieniem procedur:

- dostępu i modyfikowania do danych osobowych,
- zarządzania identyfikatorami i hasłami użytkowników,
- wykonywania kopii awaryjnych oraz odtwarzania danych z tych kopii,
- generowania wydruków danych osobowych,
- dostępu do plików rejestrujących identyfikatory oraz czas logowania użytkowników.

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

a) Wszystkie czynności związane z ich funkcjonowaniem i modernizacją.
b) Rejestrowanie i wyrejestrowywanie z systemu użytkowników oraz projektantów i programistów w czasie instalowania systemu oraz jego modyfikacji.
c) Przydzielanie uprawnień do poszczególnych funkcji systemu oraz określenie trybu i częstotliwości zmiany haseł.
d) Procedury wykonywania kopii awaryjnych, określenie ich częstotliwości, zmianę nośników oraz ich właściwe przechowywanie, sprawdzanie poprawności zapisu i likwidację.
e) Lokalizację sprzętu komputerowego, ustawienie monitorów i drukarek uniemożliwiające wgląd w dane osobom nieupoważnionym lub kradzież wymiennych nośników danych.
f) Postępowania zgodnie z instrukcją w sytuacji naruszenia ochrony danych osobowych.

Rektor
Akademii Sztuk Pięknych w Warszawie

prof. Ksawery Piwocki