Zarządzenie nr 15 /2010

Rektora Akademii Sztuk Pięknych w Warszawie

z dnia 08 kwietnia 2010 r.

w sprawie wprowadzenia zmian w Polityce Bezpieczeństwa w zakresie ochrony danych osobowych w Akademii Sztuk Pięknych w Warszawie

Zgodnie z § 3 i § 4 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, zarządzam co następuje:

§ 1

W załączniku nr 1 do Zarządzenia nr 9/2010 z dnia 02 marca 2010 r. w sprawie wprowadzenia w Akademii Sztuk Pięknych w Warszawie **Polityki Bezpieczeństwa w zakresie ochrony danych osobowych** wprowadza się następujące zmiany:

Do dotychczasowej treści **Polityki Bezpieczeństwa w zakresie ochrony danych osobowych** w Akademii Sztuk Pięknych w Warszawie dopisuje się nowy Rozdział VII o następującej treści:

„

Rozdział VII

Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

§ 23

Formy zabezpieczeń pomieszczeń, w których przetwarzane są dane osobowe:

1. wszystkie pomieszczenia, w których przetwarza się dane osobowe są zamykane na klucz, w przypadku opuszczenia pomieszczenia przez ostatnią osobę upoważnioną do przetwarzania danych osobowych – także w godzinach pracy,
2. dane osobowe przechowywane w wersji tradycyjnej (papierowej) lub elektronicznej (płyta CD, dyskietka) po zakończeniu pracy są przechowywane w zamykanych na klucz meblach biurowych, klucze od szafek należy zabezpieczyć przed dostępem osób nieupoważnionych do przetwarzania danych,
3. nieaktualne lub błędne wydruki zawierające dane osobowe niszczone są w niszczarkach.

§ 24

Formy zabezpieczeń przed nieautoryzowanym dostępem do baz danych Akademii Sztuk Pięknych w Warszawie:

1. podłączenie urządzenia końcowego (komputera, drukarki) do sieci komputerowej dokonywane jest przez administratora sieci lub upoważnionego pracownika Działu Informatycznego,
2. udostępnianie użytkownikowi zasobów zawierających dane osobowe następuje na podstawie upoważnienia do przetwarzania danych osobowych,
3. identyfikacja użytkownika w systemie poprzez zastosowanie uwierzytelnienia,
4. przydzielenie indywidualnego identyfikatora każdemu użytkownikowi systemu informatycznego i rejestrowana przez system czasu logowania użytkownika i rodzaju wprowadzonych przez niego danych,
5. serwerownia zabezpieczona przez drzwi i okna antywłamaniowe, chronione systemem alarmowym monitorowanym z zewnątrz,
6. udostępnianie kluczy i uprawnień do wejścia do serwerowni tylko pracownikom do tego upoważnionym,
7. stosowanie programu antywirusowego z zaporą antywłamaniową na komputerach ze środowiskiem operacyjnym MS Windows,
8. zabezpieczanie hasłami kont na komputerach oraz używanie kont z ograniczonymi uprawnieniami do ciągłej pracy,
9. ustawienie monitorów stanowisk przetwarzania danych osobowych w sposób uniemożliwiający wgląd w dane osobom nieupoważnionym,
10. automatyczne wygaszanie ekranu i blokowanie nieużywanego komputera po upływie określonego czasu,
11. wymuszenie zmiany hasła do systemu informatycznego co 30 dni
12. wymuszenie złożoności haseł: co najmniej 8 znaków, zawierających małe i duże litery oraz cyfry lub znaki specjalne,
13. logiczne rozdzielenie sieci wewnętrznej LAN z dostępem do baz danych oraz sieci LAN bez tego dostępu poprzez stworzenie osobnych podsieci.

§ 25

Formy zabezpieczeń przed nieautoryzowanym dostępem do baz danych Akademii Sztuk Pięknych w Warszawie poprzez Internet:

1. centralna brama sieciowa z zainstalowanym systemem typu firewall – z funkcją analizy charakteru ruchu sieciowego – uniemożliwiającym nawiązanie połączenia z chronionymi komputerami oraz blokującym ruch o charakterze niepożądanym lub takim, który może zostać uznany za szkodliwy,

2. lokalne zapory ogniowe uruchomione na wszystkich komputerach zawierających dane osobowe – uniemożliwiające nawiązanie połączenia z chronionymi komputerami oraz blokujące ruch o charakterze niepożądanym lub takim, który może zostać uznany za szkodliwy.

§ 26

Formy zabezpieczeń przed utratą danych osobowych w wyniku awarii:

1. ochrona sprzętu komputerowego, na którym przechowywane są dane osobowe przed zanikiem zasilania poprzez stosowanie zasilaczy zapasowych UPS,
2. ochrona przed utratą zgromadzonych danych poprzez cykliczne wykonywanie kopii zapasowych, z których, w przypadku awarii, odtwarzane są dane i programy służące do przetwarzania tych danych,
3. przechowywanie kopii zapasowych na nośnikach elektronicznych w osobnych pomieszczeniach w zamkniętych szafkach i usuwanie niezwłocznie po ustaniu ich użyteczności,
4. zapewnienie właściwej temperatury i wilgotności powietrza dla pracy sprzętu komputerowego w serwerowni, poprzez zastosowanie zdublowanych klimatyzatorów,
5. zastosowanie ochrony przeciwpożarowej poprzez umieszczenie w serwerowni gaśnic, okresowo kontrolowanych przez specjalistę,
6. ochrona serwerów i urządzeń sieciowych przed utratą danych spowodowaną zakłóceniami w sieci zasilającej przez zastosowanie zabezpieczeń przeciwprzepięciowych, nadprądowych i różnicowoprądowych w rozdzielni elektrycznej
7. zwiększenie niezawodności serwerów i urządzeń sieciowych poprzez logiczne rozmieszczenie ich w szafach serwerowych.

§ 27

Organizacyjną ochronę danych i ich przetwarzania realizuje się poprzez:

1. zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy ich przetwarzaniu,
2. przeszkolenie osób w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych oraz form zabezpieczenia pomieszczeń i budynków,
3. kontrolowanie pomieszczeń i budynków, w których przechowywane są dane osobowe,
4. prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
5. wyznaczenie administratora bezpieczeństwa informacji,
6. prowadzenie ewidencji zbiorów danych osobowych i programów użytkowanych do ich przetwarzania wraz z opisem struktury i sposobu przepływu tych danych pomiędzy systemami informatycznymi,

7. opracowanie i wdrożenie polityki bezpieczeństwa ASP oraz tworzenie procedur niezbędnych do ochrony danych osobowych . ”

§ 2

Zarządzenie wchodzi w życie z dniem podpisania.