Zarządzenie Nr 2
Rektora Akademii Sztuk Pięknych im. J. Matejki w Krakowie
z dnia 3 stycznia 2013 r.
w sprawie wprowadzenia w Akademii Sztuk Pięknych im. Jana Matejki w Krakowie polityki bezpieczeństwa w zakresie odnoszącym się do sposobu przetwarzania danych osobowych oraz środków ich ochrony

Na podstawie art. 66 ust. 1 ustawy z dnia 27 lipca 2005 roku Prawo o szkolnictwie wyższym (t. jedn. Dz. U. z 2012r. poz. 572 z późn. zm.), art. 36 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity z 2002 r.: Dz.U.Nr101, poz.926 z późniejszymi zmianami) w związku 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 (Dz. U. Nr 100 poz. 1024) zarządzam, co następuje:

1. Ustala się politykę bezpieczeństwa w zakresie odnoszącym się do sposobu przetwarzania danych osobowych oraz środków ich ochrony w Akademii Sztuk Pięknych im. Jana Matejki w Krakowie, stanowiącą załącznik nr 1 do niniejszego zarządzenia.
2. Ustala się Instrukcję zarządzania systemami informatycznymi w Akademii Sztuk Pięknych imienia Jana Matejki w Krakowie, stanowiącą załącznik nr 2 do niniejszego zarządzenia.
3. Ustala się Instrukcję postępowania w sytuacji naruszenia systemu ochrony danych osobowych w Akademii Sztuk Pięknych imienia Jana Matejki w Krakowie, stanowiącą załącznik nr 3 do niniejszego zarządzenia.
4. Kierujących jednostkami organizacyjnymi zobowiązuję do zapoznania podległych pracowników, którzy w ramach obowiązków przetwarzają w Akademii Sztuk Pięknych im. Jana Matejki dane osobowe, z dokumentami, o których mowa w ust. 1-3.
5. Zarządzenie wchodzi w życie z dniem podpisania.

(-) prof. Stanisław Tabisz
Rektor Akademii Sztuk Pięknych
im. Jana Matejki w Krakowie

Załącznik Nr 1 do ZARZĄDZENIA Nr 2
Rektora Akademii Sztuk Pięknych im. Jana Matejki w Krakowie
z dnia 3 stycznia 2013r.

POLITYKA BEZPIECZEŃSTWA w zakresie odnoszącym się do sposobu przetwarzania danych osobowych oraz środków ich ochrony W AKADEMII SZTUK PIĘKNYCH IMIENIA JANA MATEJKI W KRAKOWIE

Rozdział 1
Podstawa prawna
§ 1

1. Ustawa z dnia 29 sierpnia 1997 r, o ochronie danych osobowych (Dz. U. z 2002 Nr 101, póz. 926 z późniejszymi zmianami).
2. Rozporządzenie 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 (Dz. U. z 2004 r. Nr 100, póz. 1024).
3. Ustawa z dnia 12 września 1990 r. o szkolnictwie wyższym (Dz. U. Nr Nr 65, póz. 385 z późniejszymi zmianami)
4. Rozporządzenie Ministra Edukacji Narodowej i Sportu z dnia 20 września 2000 r. w sprawie dokumentacji przebiegu studiów (Dz. U. Nr 81, póz. 907 z późniejszymi zmianami).
5. Ustawa z dnia 14 marca 2003 r. o stopniach i tytule naukowym oraz o stopniach i tytule w zakresie sztuki (Dz. U. Nr 65, póz. 595).

Rozdział 2
Definicje
§ 2

Ilekroć jest mowa o:

1. zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
2. przetwarzaniu danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,

3. systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
4. zabezpieczeniu danych w systemie informatycznym - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
5. usuwaniu danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
6. administratorze danych - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3 ustawy o ochronie danych osobowych, decydujące o celach i środkach przetwarzania danych osobowych,
7. zgodzie osoby, której dane dotyczą - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści,
8. odbiorcy danych - rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
    a. osoby, której dane dotyczą,
    b. osoby upoważnionej do przetwarzania danych,
    c. przedstawiciela, o którym mowa w art. 3 la,
    d. podmiotu, o którym mowa w art. 31,
    e. organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,
9. państwie trzecim - rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego.

§ 3

Ilekroć jest mowa o:

1) ustawie - rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, zwaną dalej "ustawą";
2) identyfikatorze użytkownika - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
3) haśle - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
4) sieci telekomunikacyjnej - rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne (Dz. U. Nr 73, poz.852, z późn. zm.)
5) sieci publicznej - rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne
6) teletransmisji - rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
7) rozliczalności - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
8) integralności danych - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
9) raporcie - rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
10) poufności danych - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;

11) uwierzytelnianiu - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

Rozdział 3
Oświadczenie
§ 4

Akademia Sztuk Pięknych im. Jana Matejki w Krakowie w swojej działalności statutowej gromadzi i przetwarza dane osobowe. Dane te są wykorzystywane wyłącznie w celach określonych przez odpowiednie akty prawne, regulujące działalność publicznej szkoły wyższej. Jako państwowa jednostka organizacyjna, zgodnie z art. 7, pk. 4 ustawy, Akademia Sztuk Pięknych im. Jana Matejki w Krakowie jest administratorem danych osobowych, a ogólny nadzór nad wykonywaniem postanowień ustawy sprawuje Rektor.

Rozdział 4
Zasady ogólne
§ 5

1. Administrator danych czuwa nad zgodnym z prawem gromadzeniem danych osobowych, ich przetwarzaniem, przechowywaniem i usuwaniem, w sposób zapewniający realizację statutowych celów uczelni.
2. Administrator danych zapewnia środki techniczne i organizacyjne dla ochrony danych osobowych przetwarzanych w uczelni, w szczególności przed ich udostępnieniem osobom nieupoważnionym, przetwarzaniem z naruszeniem postanowień ustawy o ochronie danych osobowych, jak również przed utratą, uszkodzeniem lub zniszczeniem.
3. Rektor, jako administrator danych, wyznacza, dla realizacji postanowień Ustawy o ochronie danych osobowych, Administratora Bezpieczeństwa Informacji.
4. Administratorowi Bezpieczeństwa Informacji powierza się :
   a) nadzór nad bezpieczeństwem danych osobowych przetwarzanych elektronicznie i w zbiorach niezautomatyzowanych,
   b) przeciwdziałanie dostępowi do danych osobowych osobom nieupoważnionym,
   c) nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem i likwidacją,
   d) zarządzanie hasłami użytkowników,
   e) nadzór nad likwidacją nośników danych osobowych,
   f) opracowanie instrukcji zarządzania systemami informatycznymi, przetwarzającymi dane osobowe.
5. Administrator Bezpieczeństwa Informacji wnioskuje do Rektora, jako administratora danych, w sprawie wyznaczenia lokalnych administratorów danych osobowych.
6. Do gromadzenie i przetwarzania danych osobowych mogą być dopuszczone osoby, którym administrator danych wyda odpowiednie upoważnienie.
7. Rejestr osób, którym wydano upoważnienie zawiera następujące dane:
   a) imię i nazwisko osoby upoważnionej,
   b) datę nadania uprawnienia,
   c) datę ustania upoważnienia,
   d) zakres upoważnienia.
8. Osoby upoważnione są obowiązane zachować w tajemnicy dane osobowe oraz sposoby ich zabezpieczenia.
9. Imienne upoważnienia są udzielane w formie pisemnej i przechowywane w aktach osobowych pracowników.

Załączniki:

Udostępnione wraz z niniejszą instrukcją,

1. Wzór oświadczenia,
2. Wzór upoważnienia do przetwarzania danych osobowych.

Udostępnione tylko osobom upoważnionym (Administrator Bezpieczeństwa Informacji, Administrator Systemu Informatycznego oraz upoważnione przez Administratora Danych osoby):

3. Spis zbiorów danych,
4. Wykaz osób upoważnionych do przetwarzania danych osobowych,
5. Wykaz budynków, pomieszczeń w których przetwarzane są dane osobowe,

.....
/imię i nazwisko/

.....
/stanowisko/

.....
/jednostka/

OŚWIADCZENIE

Niniejszym oświadczam, iż zobowiązuję się do stosowania przepisów z zakresu ochrony danych osobowych, a w szczególności do ochrony danych osobowych przed dostępem osób nieupoważnionych, zabezpieczania ich przed zniszczeniem i nielegalnym ujawnieniem oraz do zachowania w tajemnicy powierzonych danych osobowych i sposobów ich zabezpieczenia przez cały okres wykonywania obowiązków w Akademii Sztuk Pięknych im. Jana Matejki w Krakowie (bez względu na jego podstawę), jak i po jego ustaniu.

.....
.....
/data i podpis/

Nr DK-013- /13

Pan/i
Jednostka organizacyjna

UPOWAŻNIENIE
do przetwarzania danych osobowych

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r., Nr 101, poz. 926 z późniejszymi zmianami) upoważniam **Panią/-a** do przetwarzania danych osobowych, w celach związanych z wykonywaniem obowiązków na zajmowanym stanowisku oraz pełnieniem powierzonych funkcji, w szczególności z wykorzystaniem systemu informatycznego i urządzeń wchodzących w jego skład, gdy są one przypisane do danych obowiązków.

Upoważnienie zostaje udzielone na okres zatrudnienia z możliwością wcześniejszego odwołania.

Kraków, ……..……

.....
podpis Rektora/ osoby upoważnionej

Powyższe upoważnienie przyjmuję

.....
/podpis osoby upoważnionej/

* wybrać właściwe

Załącznik Nr 2 do ZARZĄDZENIA Nr 2
Rektora Akademii Sztuk Pięknych im. Jana Matejki w Krakowie
z dnia 3 stycznia 2013r.

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI W AKADEMII SZTUK PIĘKNYCH IMIENIA JANA MATEJKI W KRAKOWIE

Rozdział 1
Przepisy ogólne
§ 1

Podstawa prawna:
1) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024)
2) ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.)

§ 2

Ilekroć w niniejszym dokumencie jest mowa o:
1) ASP– należy przez to rozumieć Akademia Sztuk Pięknych im. Jana Matejki w Krakowie;
2) Administratorze Danych – należy przez to rozumieć Rektora Akademii Sztuk Pięknych im. Jana Matejki w Krakowie;
3) Administratorze Bezpieczeństwa Informacji – należy przez to rozumieć pracownika ASP lub inną osobę wyznaczoną do nadzorowania przestrzegania zasad ochrony określonych w niniejszym dokumencie oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych;
4) Administratorze Systemu Informatycznego – należy przez to rozumieć osobę odpowiedzialną za funkcjonowanie systemu informatycznego ASP oraz stosowanie technicznych i organizacyjnych środków ochrony;
5) użytkowniku systemu – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym ASP, użytkownikiem systemu może być pracownik ASP, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w ASP lub wolontariusz;
6) sieci lokalnej – należy przez to rozumieć połączenie systemów informatycznych ASP wyłącznie dla własnych jej potrzeb przy wykorzystaniu urządzeń i sieci Telekomunikacyjnych;
7) sieci rozległej – należy przez to rozumieć sieć publiczną w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z późn. zm.).

Rozdział 2

Procedury nadawania i zmiany uprawnień do przetwarzania danych

§ 3

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych ma obowiązek zapoznać się z:
   1) ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.);
   2) rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024),
   3) polityką bezpieczeństwa w zakresie odnoszącym się do sposobu przetwarzania danych osobowych oraz środków ich ochrony stanowiącą załącznik do nr 1 do zarządzenia nr 2 Rektora Akademii Sztuk Pięknych im. Jana Matejki w Krakowie z dnia 3 stycznia 2013r.
   4) niniejszą instrukcją,
   5) instrukcją postępowania w sytuacji naruszenia systemu ochrony danych osobowych stanowiącą załącznik do nr 3 do zarządzenia nr 2 Rektora Akademii Sztuk Pięknych im. Jana Matejki w Krakowie z dnia 3 stycznia 2013r.
2. Administrator Bezpieczeństwa Informacji przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie upoważnienia/wniosku Administratora Danych określającego zakres uprawnień pracownika.
3. Wykaz osób upoważnionych do przetwarzania danych osobowych winien odzwierciedlać aktualny stan systemu w zakresie użytkowników i ich uprawnień.
4. Wykaz osób upoważnionych do przetwarzania danych osobowych w systemach informatycznych powinien zawierać:
   1) imię i nazwisko użytkownika systemów informatycznych;
   2) rodzaj uprawnienia;
   3) datę nadania uprawnienia;
   4) datę odebrania uprawnienia;
   5) przyczynę odebrania uprawnienia;
   6) podpis Administratora Bezpieczeństwa Informacji.
5. Wzór rejestru użytkowników i ich uprawnień w systemach informatycznych w Akademii Sztuk Pięknych im. Jana Matejki w Krakowie związanych z przetwarzaniem danych osobowych stanowi załącznik do instrukcji.
6. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora, hasła oraz zakresu dostępnych danych i operacji. Ustanowione hasło, Administrator Systemu Informatycznego przekazuje użytkownikowi ustnie.
7. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.
8. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
9. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako naruszenie podstawowych obowiązków pracowniczych.
10. Pracownik zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest do zachowania ich w tajemnicy. Tajemnica obowiązuje go również po ustaniu zatrudnienia.
11. Jeżeli to tylko możliwe w systemie informatycznym stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do sieci lokalnej oraz dostępu do aplikacji.

12. Identyfikator użytkownika w aplikacji (o ile działanie aplikacji na to pozwala), powinien być tożsamy z tym, jaki jest mu przydzielany w sieci lokalnej.
13. Odebranie uprawnień pracownikowi następuje na pisemny wniosek kierownika, któremu pracownik podlega z podaniem daty oraz przyczyny odebrania uprawnień. Odebranie uprawnień pracownikowi równoważne jest z usunięciem lub zablokowaniem konta w systemie informatycznym.
14. Kierownicy komórek organizacyjnych zobowiązani są pisemnie informować Administratora Bezpieczeństwa Informacji o każdej zmianie dotyczącej podległych pracowników mającej wpływ na zakres posiadanych uprawnień w systemie informatycznym.
15. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane oraz unieważnić jej hasło.
16. Administrator Bezpieczeństwa Informacji zobowiązany jest do prowadzenia i ochrony rejestru użytkowników i ich uprawnień w systemie informatycznym.

Rozdział 3

Zasady posługiwania się hasłami

§ 4

1. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i hasła.
2. Hasło powinno być zmieniane przez użytkownika, co najmniej raz w miesiącu.
3. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po Wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.
4. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł.
5. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
6. Pracownik nie ma prawa do udostępniania haseł.
7. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
8. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła.
9. Przy wyborze hasła obowiązują następujące zasady:
   1) minimalna długość hasła - 8 znaków;
   2) zakazuje się stosować:
      a) haseł, które użytkownik stosował uprzednio w okresie minionego roku,
      b) swojej nazwy użytkownika w jakiejkolwiek formie (pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę, itp.),
      c) swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiejkolwiek formie,
      d) imion (w szczególności imion osób z najbliższej rodziny),
      e) ogólnie dostępnych informacji o użytkowniku takich jak: numer telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego, nazwa ulicy, na której mieszka lub pracuje, itp.,
      f) wyrazów słownikowych,
      g) przewidywalnych sekwencji znaków z klawiatury np.: QWERTY", "12345678", itp.,
      h) identyfikatorem użytkownika;
   3) należy stosować:
      a) hasła zawierające kombinacje liter i cyfr,

b) hasła zawierające znaki specjalne: znaki interpunkcyjne, nawiasy, symbole @, #, &, itp., o ile system informatyczny na to pozwala,
c) hasła, które można zapamiętać bez zapisywania,
d) hasła łatwe i szybkie do wprowadzenia, po to by trudniej było podejrzeć je osobom trzecim.

10. Zmiany hasła nie wolno zlecać innym osobom.
11. W systemach, które umożliwiają opcję zapamiętania nazw użytkownika lub jego hasła nie należy korzystać z tego ułatwienia.
12. Hasło użytkownika o prawach administratora powinno znajdować się w zalakowanej kopercie w zamykanej na klucz szafie metalowej, do której dostęp mają:
    1) Administrator Bezpieczeństwa Informacji;
    2) Administrator Danych;
    3) Administrator Systemu Informatycznego.

Rozdział 4

Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie

§ 5

1. Przed rozpoczęciem pracy w systemie komputerowym należy zalogować się do systemu przy użyciu indywidualnego identyfikatora oraz hasła.
2. Przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wykonać opcję wylogowania z systemu (zablokowania dostępu), lub jeżeli taka możliwość nie istnieje wyjść z programu.
3. Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązana jest wykonać funkcję wylogowania z systemu.
4. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów, wykonać zamknięcie systemu i jeżeli jest to konieczne wylogować się z sieci komputerowej
5. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania oraz zakończeniem pracy w sieci.

Rozdział 5

Procedury tworzenia zabezpieczeń

§ 6

1. Za systematyczne przygotowanie kopii bezpieczeństwa danych przechowywanych na serwerze odpowiada Administrator Systemu Informatycznego. Za kopie bezpieczeństwa danych przechowywanych na komputerach lokalnych odpowiada użytkownik, któremu sprzęt został powierzony do pracy.
2. Kopie bezpieczeństwa danych przechowywanych na serwerach wykonywane są codzienne po zakończeniu pracy wszystkich użytkowników. Kopie danych przechowywanych na komputerze lokalnym powinny być wykonywane nie rzadziej niż raz w tygodniu.

Rozdział 6

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz wydruki

§ 7

1. Elektroniczne nośniki informacji:
   1) dane osobowe w postaci elektronicznej - za wyjątkiem kopii bezpieczeństwa – zapisane na dyskietkach, dyskach magnetooptycznych czy dyskach twardych nie są wynoszone poza siedzibę ASP;
   2) wymienne elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych. Wykaz budynków i pomieszczeń tworzących obszary, w których przetwarzane są dane osobowe stanowi załącznik do polityki bezpieczeństwa;
   3) po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki informacji są przechowywane w zamykanych szafach biurowych lub kasetkach;
   4) urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się fizycznie w sposób uniemożliwiający ich odczytanie;
   5) urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej.

2. Kopie zapasowe:
   1) kopie zapasowe zbioru danych osobowych oraz oprogramowania i narzędzi programowych zastosowanych do przetwarzania danych są przechowywane w serwerowni, pok. 502 oraz w Głównym Punkcie Dystrybucyjnym: pok. 504, pl. Matejki 13;
   2) dostęp do danych opisanych w punkcie 1 ma Administrator Bezpieczeństwa Informacji Administrator Systemu Informatycznego oraz upoważnieni przez Administratora Danych pracownicy.

3. Wydruki:
   1) w przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym;
   2) pomieszczenie, w którym przechowywane są wydruki robocze musi być należycie zabezpieczone po godzinach pracy;
   3) wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

Rozdział 7

Środki ochrony systemu przed złośliwym oprogramowaniem, w tym wirusami komputerowymi

§ 8

1. Na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe pracujące w trybie monitora.
2. Każdy e-mail musi być sprawdzony pod kątem występowania wirusów przez program antywirusowy.
3. Definicje wzorców wirusów aktualizowane są kilka razy w czasie dnia.
4. Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje użytkownik, który nośnik zamierza użyć.
5. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.
6. Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje pracownik, który pocztę otrzymał.
7. Administrator Systemu Informatycznego przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach.
8. Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania.
9. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe, na którym wirusa wykryto.

Rozdział 8

Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych

§ 9

1. Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie osobom upoważnionym.
2. Udostępnienie danych osobowych w jakiejkolwiek postaci, wymaga pisemnego upoważnienia Administratora Danych.
3. Udostępnienie danych osobowych nie może być realizowane drogą telefoniczną. Droga elektroniczna jest dopuszczalna pod warunkiem zastosowania odpowiednich poziomów szyfrowania i certyfikacji by mieć pewność, iż dane nie zostaną odczytane przez osoby do tego nieupoważnione.
4. Udostępnienie danych osobowych następuje po przedstawieniu wniosku wg wzoru określonego w załączniku do instrukcji.
5. Pracownicy prowadzą rejestry udostępnionych danych osobowych zawierające, co najmniej: datę udostępnienia, podstawę, zakres udostępnionych informacji oraz osobę lub instytucję, dla której dane udostępniono.
6. Aplikacje wykorzystywane do obsługi baz danych osobowych powinny zapewniać odnotowanie informacji o udzielonych odbiorcom danych. Zakres informacji powinien obejmować, co najmniej: dane odbiorcy, datę wydania, zakres udostępnionych danych.

Rozdział 9

Postępowanie w sytuacji naruszenia ochrony danych osobowych

§ 10

Postępowanie w sytuacji naruszenia ochrony danych osobowych określa Instrukcja regulująca postępowanie pracowników Akademii Sztuk Pięknych im. Jana Matejki w Krakowie zatrudnionych przy przetwarzaniu danych osobowych w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych.

Rozdział 10

Procedury wykonywania przeglądów i konserwacji systemu

§ 11

1. Przeglądy i konserwacja urządzeń:
   1) przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonym przez producenta sprzętu;
   2) nieprawidłowości ujawnione w trakcie tych działań powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. O fakcie ujawnienia nieprawidłowości należy zawiadomić Administratora Bezpieczeństwa Informacji.

2. Przegląd programów i narzędzi programowych:
   1) konserwacja baz danych przeprowadzana jest zgodnie z zaleceniami twórców poszczególnych programów;
   2) Administrator Bezpieczeństwa Informacji zobowiązany jest uaktywnić mechanizm zliczania nieudanych prób zameldowania się do systemu oraz ustawić blokadę konta użytkownika po wykryciu trzech nieudanych prób, we wszystkich systemach posiadających taką funkcję o ile system informatyczny to umożliwia;
   3) wszystkie logi opisujące pracę systemu, zameldowania i wymeldowania użytkowników oraz rejestr z systemu śledzenia wykonywanych operacji w programie należy przed usunięciem zapisać na płytę CD-R/DVD-R.

Rozdział 11

Połączenie do sieci Internet

§12

Połączenie lokalnej sieci komputerowej ASP z Internetem jest dopuszczalne wyłącznie po zainstalowaniu mechanizmów ochronnych (firewall) oraz kompleksowego oprogramowania antywirusowego.

Rozdział 12

Postanowienia końcowe

§ 13

Na stanowisku pracy obowiązuje zakaz instalowania jakiegokolwiek oprogramowania bez uzgodnienia z Administratorem Systemu Informatycznego. Pracownik chcąc zainstalować aplikację lub program musi uzyskać pisemną zgodę od Administratora Systemu Informatycznego.

Załączniki:

Udostępnione wraz z niniejszą instrukcją:

1. Wzór rejestru użytkowników i ich uprawnień w systemach informatycznych,
2. Wzór wniosku o udostępnienie danych osobowych.

Udostępnione tylko osobom upoważnionym (Administrator Bezpieczeństwa Informacji, Administrator Systemu Informatycznego oraz upoważnieni przez Administratora Danych pracownicy):

3. Rejestr użytkowników i ich uprawnień w systemach informatycznych

Rejestr użytkowników i ich uprawnień w systemach informatycznych.

Zbiór danych:……………………………………………………………………….
ostatnia aktualizacja:………………………..

lp	*imię*	*nazwisko*	*identyfikator*	*data nadania dostępu*	*data ustania dostępu*	*uprawnienia*	*uwagi*

Wniosek o udostępnienie danych ze zbioru danych osobowych

1.Wniosek do Akademii Sztuk Pięknych im. Jana Matejki w Krakowie, pl. Matejki 13, 31-157 Kraków

(dokładne oznaczenie administratora danych)

2.Wnioskodawca

……
……
……
……
……

(nazwa firmy i jej siedziba albo nazwisko, imię i adres zamieszkania wnioskodawcy)

3.Podstawa prawna upoważniająca do pozyskania danych albo wskazania wiarygodnie uzasadnionej potrzeby posiadania danych w przypadku osób innych niż wymienione w art.29 ust. 1 Ustawy o danych osobowych

……
……
.....
.....
.....
.....
.....□...* ew. cd w załączniku nr.....

4. Wskazanie przeznaczenia dla udostępnionych danych

.....
.....□....* ew. cd w załączniku nr.....

5. Oznaczenie lub nazwa zbioru, z którego mają być udostępnione dane

.....
.....
.....
.....
.....

6. Zakres żądanych informacji ze zbioru…….....

.....

.....

.....

.....

.....□....* ew. cd w załączniku nr.....

7. Informacje umożliwiające wyszukiwanie w zbiorze danych

.....

.....

.....

.....□....* ew. cd w załączniku nr....

UWAGA ! : Otrzymane dane mogą być wykorzystane wyłącznie do celów wskazanych we wniosku .

Należność..... .....

.....

(data , podpis ew. pieczęć wnioskodawcy)

Pokwitowanie nr.....

Kwituję odbiór dnia .....

* Jeśli tak to zakreśl kwadrat literą “x”

.....

(podpis)

Załącznik Nr 3 do ZARZĄDZENIA Nr 2
Rektora Akademii Sztuk Pięknych im. Jana Matejki w Krakowie
z dnia 3 stycznia 2013r.

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA SYSTEMU OCHRONY DANYCH OSOBOWYCH W AKADEMII SZTUK PIĘKNYCH IMIENIA JANA MATEJKI W KRAKOWIE

Rozdział 1
.Postanowienia ogólne
§ 1

1. Instrukcję opracowano na podstawie:
   1) ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2002r. Nr 101 poz. 926, ze zm.),
   2) 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 (Dz. U. Nr 100 poz. 1024),
   3) wewnątrzuczelnianych regulacji dotyczących ochrony danych osobowych.
2. Instrukcja niniejsza określa tryb i zasady postępowania wszystkich pracowników Akademii Sztuk Pięknych im. Jana Matejki w Krakowie, a w szczególności osób zatrudnionych przy przetwarzaniu danych osobowych, w przypadku, gdy: zabezpieczenia systemu informatycznego, stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń danych.
3. Osobą odpowiedzialną za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe jest Administrator Systemu Informatycznego.
4. Źródłem informacji o sprawności systemów ochrony jest stały ich monitoring oraz wszelkie zgłoszenia stwierdzające nieprawidłowości w pracy systemu informatycznego.
5. Każda informacja o naruszeniu systemu bezpieczeństwa , pochodząca z jakiegokolwiek źródła wymaga od Administratora Bezpieczeństwa Informacji wszczęcia postępowania wyjaśniającego, aby określić:
   1) czas, charakter, miejsce, sposób i skutki naruszenia systemu zabezpieczeń,
   2) w jaki sposób usunąć lub zminimalizować skutki,
   3) jakie dodatkowe środki należy zastosować w celach profilaktycznych,
   4) sprawcę i cel, gdy istnieje ku temu możliwość.

6. Zagrożenie bezpieczeństwa danych osobowych może wystąpić w:
   1) miejscu przetwarzania danych na sprzęcie komputerowym,
   2) oprogramowaniu,
   3) ręcznych zbiorach danych osobowych.
7. Sposób naruszenia bezpieczeństwa to przede wszystkim:
   1) osłabienie odporności systemu zabezpieczeń, w szczególności tworzenie potencjalnych zagrożeń dla systemu (np. niezamykanie pomieszczeń, sejfów, pozostawianie dokumentacji, lub otwartego dostępu do aplikacji na opuszczonym stanowisku pracy.
   2) nieuzasadnione wynoszenie dokumentacji z miejsca pracy, samowolna instalacja niedozwolonych programów i sprzętu na osobistych stanowiskach pracy itp.), nieuprawnione „przeglądanie", sporządzanie notatek, wyciągów raportów, kopii, itp.,
   3) zmiana zawartości zgromadzonych danych naruszająca ich integralność, wiarygodność, usunięcie całości bądź części danych lub ich uszkodzenie,
   4) fizyczne zniszczenie zasobów, kradzież sprzętu, oprogramowania,
   5) przekazanie zgromadzonych danych osobom nieuprawnionym.
8. Naruszenie systemu zabezpieczeń może mieć charakter:
   1) wewnętrzny lub zewnętrzny,
   2) incydentalny lub chroniczny,
   3) nieświadomy lub zamierzony.

Rozdział 2
Tryb i zasady postępowania w przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego
§ 2

1. Każdy pracownik, w szczególności użytkownik systemu informatycznego, po stwierdzeniu
   naruszenia zabezpieczenia systemu informatycznego (włamania do systemu) ma obowiązek
   niezwłocznie powiadomić o tym bezpośredniego przełożonego - lokalnego administratora danych osobowych - zwanego dalej kierownikiem jednostki organizacyjnej.
2. Kierownik jednostki organizacyjnej zawiadamia niezwłocznie Administratora Bezpieczeństwa Informacji, który podejmuje niezbędne działania pozwalające na ustalenie
   okoliczności naruszenia systemu informatycznego oraz zapobieżenia jego skutkom w tym przede wszystkim:
   zleca Administratorowi Systemu Informatycznego wykonanie czynności mających na celu:
   1) uniemożliwienie dalszego naruszenia zabezpieczenia systemu,
   2) zabezpieczenie i utrwalenie wszelkich informacji i dokumentów mogących stanowić pomoc przy ustaleniu przyczyn naruszenia,
   3) ustalenie charakteru i rodzaju naruszenia oraz ewentualnych metod działania osób naruszających zabezpieczenie systemu.
   4) przywrócenie prawidłowego stanu działania systemu, a w przypadku uszkodzenia baz danych, odtworzenie ich z ostatnich kopii awaryjnych z zachowaniem należytych środków ostrożności,
   5) dokonanie analizy stanu systemu wraz z oszacowaniem rozmiaru szkód powstałych na skutek naruszenia.

Rozdział 3

Tryb postępowania w przypadku podejrzenia naruszenia zabezpieczeń danych osobowych spowodowanego stanem technicznym urządzeń, sposobem działania programu, jakością komunikacji w sieci telekomunikacyjnej, naruszeniem zawartości ręcznego zbioru danych osobowych

§ 3

1. Pracownik Akademii Sztuk Pięknych im. Jana Matejki w Krakowie, w szczególności zatrudniony przy przetwarzaniu danych osobowych, w przypadku podejrzenia naruszenia zabezpieczeń danych osobowych, obowiązany jest niezwłocznie powiadomić o tym kierownika jednostki organizacyjnej.
2. Kierownik jednostki organizacyjnej zawiadamia niezwłocznie Administratora Bezpieczeństwa Informacji, który zleca Administratorowi Sytemu Informatycznego:
   1) sprawdzenie stanu urządzeń wykorzystywanych do przetwarzania danych osobowych;
   2) kontrolę sposobu działania programu (w tym również obecność wirusów komputerowych);
   3) sprawdzenie jakość komunikacji w sieci telekomunikacyjnej;
   4) sprawdzenie zawartości zbioru danych osobowych w systemie informatycznym,
   5) podjęcie dalszych działań zgodnie z § 2 ust. 2.
3. Administrator Bezpieczeństwa Informacji wraz z kierownikiem jednostki organizacyjnej sprawdzają (jeśli zaistnieje taka konieczność) zawartość ręcznych zbiorów danych i ustalają czy nie doszło do naruszenia zabezpieczeń technicznych (tzn. wyłamanie zamków,
   wyważenie drzwi itp.), a także czy nie nastąpiło zaniedbanie ze strony pracownika, które mogło doprowadzić do naruszenia ochrony danych osobowych.

Rozdział 4

Dokumentacja faktu naruszenia systemu zabezpieczenia danych osobowych

§ 4

1. Administrator Bezpieczeństwa Informacji sporządza szczegółowy protokół zawierający w szczególności: datę i godzinę otrzymania informacji o naruszeniu (włamaniu do systemu), opis jego przebiegu, przyczyny zdarzenia, dowody dokumentujące naruszenie systemu, oraz wnioski. Protokół przekazuje Administratorowi Danych Osobowych (Rektorowi).
2. Jeśli w wyniku naruszenia zabezpieczeń lub zakłócenia pracy sytemu nastąpiło ujawnienie danych osobowych osobie nieuprawnionej, Rektor niezwłocznie powołuje komisję dla pełnego zbadania skutków przestępstwa, ustalenia sprawcy i stopnia jego winy oraz wielkości poniesionych strat. Ustalenia komisji są podstawą do ewentualnego wszczęcia postępowania wobec winnych oraz minimalizacji i naprawy poniesionych szkód, a także działań eliminujących takie zdarzenia w przyszłości.
3. Tryb ten obowiązuje również w razie stwierdzenia świadomego uszkodzenia, zniszczenia bądź bezzasadnej modyfikacji zasobów, nawet wówczas, gdy nie zostały one udostępnione osobom nieuprawnionym do ich posiadania.
4. Zakończeniem postępowania wyjaśniającego jest sporządzenie protokołu podpisanego przez członków komisji.

Rozdział 5
Działania profilaktyczne
§ 5

1. W przypadku naruszenia zabezpieczeń systemu informatycznego lub ręcznych zbiorów danych osobowych Administrator Bezpieczeństwa Informacji, wspólnie z Administratorem Systemu Informatycznego i w porozumieniu z kierownikami jednostek organizacyjnych Akademii Sztuk Pięknych im. Jana Matejki w Krakowie podejmą działania w celu zapobieżenia takim faktom w przyszłości.
2. Administrator Bezpieczeństwa Informacji po porozumieniu z kierownikiem jednostki organizacyjnej podejmuje niezbędne działania/lub zleca ich podjęcie/ w celu zapobieżenia naruszeniom zabezpieczeń systemu informatycznego w przyszłości. Jeżeli przyczyną zdarzenia był stan techniczny urządzenia, sposób działania programu, uaktywnienie się wirusa komputerowego lub jakość komunikacji w sieci telekomunikacyjnej Administrator Systemu Informatycznego ma obowiązek niezwłocznie przeprowadzić, w stosownym zakresie, przeglądy oraz konserwacje urządzeń i programów, ponadto zobowiązany jest do
   ustalenia źródła pochodzenia wirusa oraz wdrożenia skuteczniejszych programów antywirusowych.
3. W przypadku, gdy przyczyną zdarzenia były wadliwe metody pracy, błędy i zaniedbania osób zatrudnionych przy przetwarzaniu danych osobowych Administrator Bezpieczeństwa Informacji wraz Administratorem Systemu Informatycznego przeprowadzą dodatkowe szkolenia osób biorących udział przy przetwarzaniu danych.

Rozdział 6
Postanowienia końcowe
§ 6

Każda osoba wpisana do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych zobowiązana jest do zapoznania się z niniejszą instrukcją.