POLITYKA BEZPIECZEŃSTWA INFORMACJI

AKADEMII SZTUK PIĘKNYCH W GDAŃSKU

W OPARCIU O NORMĘ

PN-ISO/IEC 17799:2007 i 27001:2007

SPIS TREŚCI

Część Pierwsza - Ogólna

POLITYKA BEZPIECZEŃSTWA INFORMACJI

W OPARCIU O NORMĘ PN-ISO/IEC 17799:2007 i 27001:2007

Wprowadzenie

W coraz większym stopniu instytucje, ich systemy i sieci informatyczne stają w obliczu zagrożeń pochodzących z rozmaitych źródeł, takich jak oszustwa dokonywane za pomocą komputerów, komunikatorów, urządzeń mobilnych oraz sieci. Maskarady, szpiegostwo, sabotaż, wandalizm, pożar lub powódź to zjawiska aktywnej lub losowej utraty informacji oraz danych. Odpowiednie zabezpieczenia, ochrona przetwarzanych danych, niezawodność funkcjonowania oraz systematyczna i wielowątkowa organizacja edukacji użytkowników stają się podstawowymi wymogami stawianymi współczesnym systemom informatycznym, a informacja oraz wspierające ją procesy, systemy i sieci są ważnymi aktywami działalności każdej jednostki organizacyjnej.

Jednym słowem poufność, dostępność i integralność informacji ma podstawowe znaczenie dla utrzymania konkurencyjności, płynności finansowej, zysku i zgodności z przepisami prawa oraz wizerunku jednostki.

W związku z powyższym oraz 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 (Dz. U. Nr 100 poz. 1024), administrator danych obowiązany jest do opracowania (w formie pisemnej) i wdrożenia polityki bezpieczeństwa.

Pojęcie „polityka bezpieczeństwa", użyte w rozporządzeniu należy rozumieć, jako zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji wrażliwej (tutaj danych osobowych) wewnątrz organizacji.[1]

Dokument zwraca uwagę na konsekwencje, jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń. Jednocześnie deklaruje zaangażowanie kierownictwa i wyznacza procesowe podejście instytucji do zarządzania bezpieczeństwem informacji. Ponadto niektóre zabezpieczenia opisane w niniejszym dokumencie są traktowane jako zasady przewodnie w zarządzaniu bezpieczeństwem informacji, możliwe do zastosowania i zapewniające odpowiedni punkt wyjścia dla procesu wdrażania bezpieczeństwa informacji.

Omawiane zasady opierają się na obowiązujących uregulowaniach prawnych, a należą do nich w szczególności:

a) ochrona danych osobowych i prywatności osób;
b) ochrona dokumentów instytucji; prawa własności intelektualnej;
c) dokumenty polityki bezpieczeństwa informacji;

[1] 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. Nr 100, poz. 1024)

d) odpowiedzialność związana z bezpieczeństwem informacji;
e) edukacja w dziedzinie bezpieczeństwa informacji;
f) wsparcie i zaangażowanie kadry kierowniczej;
g) upowszechnianie wytycznych dotyczących polityki bezpieczeństwa informacji wśród wszystkich użytkowników;
h) zgłaszanie przypadków naruszenia bezpieczeństwa.[2]

Głównym celem POLITYKI BEZPIECZEŃSTWA INFORMACJI (PBI) stosowanej w bieżącej działalności Akademii Sztuk Pięknych jest organizacyjne, fizyczne i logiczne zabezpieczenie posiadanych zasobów danych osobowych, oraz systematyczne edukowanie użytkowników systemu ochrony danych osobowych. Odpowiedzialność za realizacje ochrony danych ponoszą WSZYSCY UŻYTKOWNICY w zakresie proporcjonalnie nadanych uprawnień. PBI jest jednocześnie materiałem określającym zadania w zakresie właściwej realizacji poufności i integralności danych osobowych przez nadanie uprawnień legalizujących przetwarzanie danych użytkownikom systemu ochrony informacji.

Rozdział I

Przepisy ogólne, definicje oraz objaśnienia

§1

Polityka Bezpieczeństwa Informacji uwzględnia wymagania dotyczące zarządzania bezpieczeństwem informacji zawarte w Normie PN-ISO/IEC 17799:2007 i 27001:2007 oraz w poniższych dokumentach:

a) Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997r. (Dz. U. nr 101, poz. 926 z późn. zmian.);
b) 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);
c) Norma PN - ISO/IEC 17799:2007 Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji;
d) Norma PN ISO/IEC 27001:2007 Technika informatyczna. Techniki bezpieczeństwa Systemy zarządzania bezpieczeństwem informacji Wymagania.

Powyższe normy wskazują warunki oraz zalecenia w zakresie zarządzania bezpieczeństwem informacji do wykorzystania przez wszystkich tych, którzy są odpowiedzialni za inicjowanie, wdrażanie oraz utrzymywanie bezpieczeństwa w organizacji, którą jest Akademia Sztuk Pięknych. Zamiarem administratora zarządzającego bezpieczeństwem informacji, jest dostarczenie wszystkim użytkownikom możliwie najpełniejszej wiedzy w celu ujednolicenia norm bezpieczeństwa i efektywnej praktyki zarządzania bezpieczeństwem informacji oraz zapewnienie zaufania w stosunkach pomiędzy współpracującymi z Akademią Sztuk Pięknych organizacjami i klientami.

- dane osobowe – to w rozumieniu ustawodawcy, wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, wykorzystywane w procesach przetwarzania danych osobowych w Akademii

[2] ISO/IEC 17799 - Technika informatyczna - Praktyczne zasady zarządzania bezpieczeństwem informacji

Sztuk Pięknych. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny [PESEL], albo jeden z kilku specyficznych czynników określających jej cechy:

- fizyczne, wizerunek;
- zdrowia, orzeczenia i zaświadczenia lekarskie;
- fizjologiczne;
- umysłowe;
- ekonomiczne;
- kulturowe lub społeczne

Wykorzystanie danych osobowych w procesach przetwarzania może obejmować inne dane w granicach określonych odrębnymi przepisami prawa.

- zbiór danych osobowych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony (jego części znajdują się w różnych miejscach) lub podzielony funkcjonalnie (przetwarzany za pomocą programów realizujących zróżnicowane funkcje; tworzone doraźnie lub do celów techniczno – szkoleniowych, rekrutacyjnych, działalności Uczelnianej Komisji Rekrutacyjnej i innych działów organizacyjnych); wykorzystywany w bieżącej pracy komórek organizacyjnych Akademii Sztuk Pięknych;
- przetwarzanie danych osobowych - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, udostępnianie i usuwanie; zwłaszcza takie, które wykorzystuje się w systemach informatycznych;
- system informatyczny - system przetwarzania informacji realizowany w Akademii Sztuk Pięknych, wraz ze związanymi z nimi ludźmi oraz zasobami technicznymi i finansowymi, który dostarcza i rozprowadza informacje. Ochronie podlegają nie tylko informacje osobowe, ale także użytkownicy, zasoby techniczne [stacjonarne i mobilne urządzenia i nośniki] oraz metody ochrony informacji, oraz wiedza Wykonawcy procesu nadzoru technicznego w zakresach przetwarzanych danych w Akademii Sztuk Pięknych;
- bezpieczeństwo systemu informatycznego – wdrożenie odpowiednich środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów informacyjnych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub nieuprawnionym pozyskaniem danych osobowych, a także ich utratą (zamierzoną lub przypadkową);
- administrator Danych Osobowych (ADO) - organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych; administratorem Danych Osobowych jest Akademia Sztuk Pięknych reprezentowana przez Rektora Akademii Sztuk Pięknych w Gdańsku lub osobę przez Rektora upoważnioną, który ponosi pełnię odpowiedzialności wynikającej z przepisów ustawy o ochronie danych osobowych w odniesieniu do zbiorów danych osobowych znajdujących się w jego ustawowej i statutowej dyspozycji;
- administrator Bezpieczeństwa Informacji (ABI) ASP w Gdańsku - należy przez to rozumieć osobę / podmiot (uprawnionych reprezentantów) wyznaczoną przez Administratora Danych Osobowych do nadzorowania przestrzegania zasad ochrony oraz wymagań w zakresie ochrony, wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych;
- administrator Systemów Informatycznych (ASI) ASP w Gdańsku - należy przez to rozumieć wykonawcę (uprawnionych przedstawicieli) z zakresu

informatyki odpowiedzialnego za stosowanie technicznych i organizacyjnych środków ochrony danych osobowych w systemach informatycznych;

- użytkownik – osoba posiadająca upoważnienie wydane przez ADO i uprawniona do przetwarzania danych osobowych w odpowiedniej komórce organizacyjnej, lub zgodnie z umową zlecenia / o dzieło w zakresie wskazanym w upoważnieniu;
- identyfikator użytkownika (LOGIN) - ciąg znaków literowych i cyfrowych, lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym ASP w Gdańsku;
- hasło (Password) - ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
- zalogowanie - uwierzytelnienie czyli działanie, którego celem jest weryfikacja deklarowanej tożsamości użytkownika / podmiotu;
- odbiorcy danych osobowych - rozumie się przez to każdego dostawcę usługi, a także podmiot któremu udostępnia się dane osobowe, z wyłączeniem:
  - osoby, której dane dotyczą;
  - osoby, upoważnionej do przetwarzania danych;
  - przedstawiciela, o którym mowa w art. 31 a ustawy o ochronie danych osobowych;
  - podmiotu, o którym mowa w art. 31 ustawy o ochronie danych osobowych;
  - organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

Polityka Bezpieczeństwa Informacji w uporządkowanej formie opisuje działania organizacyjne i techniczne, których celem jest zapewnienie bezpieczeństwa danych osobowych w ASP w Gdańsku, oraz w relacjach powierzania danych osobowych wykonawcom w ramach realizowanych projektów lub umów.
Polityka Bezpieczeństwa Informacji ustala zakresy obowiązków osób i innych organizacji w procesie obiegu i ochrony informacji. Określa cel i zakres przetwarzanych danych osobowych w indywidualnych umowach z podmiotami zewnętrznymi, którym zlecono przetwarzanie danych osobowych.

§2

1. Dostęp do zbioru danych osobowych oraz ich przetwarzania posiadają wyłącznie osoby wpisane do Rejestru wydanych upoważnień prowadzonego przez Administratora Bezpieczeństwa Informacji.
2. Osoby zaangażowane w procesie przetwarzania danych osobowych są zobowiązane do przechowywania danych osobowych we właściwych zbiorach i wszelkich nośnikach, nie dłużej niż jest to niezbędne dla osiągnięcia celu ich przetwarzania. Użytkownicy zaangażowani w procesie przetwarzania danych osobowych w systemach informatycznych zobowiązani są do postępowania zgodnie z „Instrukcją Zarządzania Systemem Informatycznym".

§3

Użytkownicy przetwarzający dane osobowe zobowiązani są do informowania Administratora Bezpieczeństwa Informacji o ewentualnych incydentach/ naruszeniach

lub utracie [nośniki] bezpieczeństwa systemu ochrony danych osobowych we wszystkich administrowanych zbiorach. Tryb postępowania określa rozdział pomocniczy - „Instrukcja postępowania w sytuacjach naruszenia ochrony danych osobowych".

§4

Użytkownik który przetwarza w zbiorze danych dane osobowe, do których przetwarzania nie jest upoważniony - podlega odpowiedzialności karnej zgodnie z Ustawą o ochronie danych osobowych oraz dyscyplinarnej określonej przepisami Kodeksu Pracy.

Rozdział II

Gromadzenie danych osobowych

§1

Dane osobowe przetwarzane w Akademii Sztuk Pięknych w Gdańsku mogą być uzyskiwane:

1. Bezpośrednio od osób, których te dane dotyczą, w zakresie:
   a) spełnienia obowiązku wynikającego z przepisów prawa;
   b) oświadczenia woli.
2. Z innych źródeł, w granicach dozwolonych przepisami prawa [sądy; prokuratura].

§2

Zbierane dane osobowe mogą być wykorzystane wyłącznie do celów, w jakich są lub będą przetwarzane. Po wykorzystaniu danych osobowych, powinny być one przechowywane w postaci uniemożliwiającej identyfikację osób, których dotyczą (anonimizacja danych).

Rozdział III

Obowiązek informacyjny

§1

1. Akademia Sztuk Pięknych w Gdańsku odpowiedzialna jest za poinformowanie osób, których dane przetwarza o:
   a) Adresie siedziby, gdzie są zbierane i przetwarzane;
   b) Celu zbierania danych, dobrowolności lub obowiązku podania danych, a jeżeli taki obowiązek istnieje, oraz jego podstawie prawnej;
   c) Prawie dostępu do treści swoich danych osobowych oraz ich poprawienia.
2. Obowiązek spełniany jest poprzez komunikat umieszczony na stronie Biuletynu Informacji Publicznej i tablicach ogłoszeń Akademii Sztuk Pięknych w Gdańsku.
3. W przypadku zbierania danych osobowych nie od osób, których one dotyczą, osoby których dotyczą należy poinformować ponadto o:

a) Źródle danych;
b) Uprawnieniach wynikających z art. 32 ust. 1 pkt. 7 i 8 ustawy o ochronie danych osobowych (prawie do wniesienia sprzeciwu).

§2

Materiały dotyczące działalności (wszelkie rodzaje inicjatyw korespondencyjnych jak – przesyłki, ulotki promocyjne, zaproszenia, kariera absolwenta/ów) mogą być wysłane wyłącznie do tych osób, które wcześniej wyraziły zgodę na piśmie na przetwarzanie ich danych osobowych w tym celu. Konieczność wyrażania zgody nie dotyczy osób reprezentujących podmioty współpracujące z Akademią Sztuk Pięknych w Gdańsku.

Rozdział IV

Udzielanie informacji o przetwarzaniu danych osobowych

§1

1. Osobom, których dane przetwarza się w zbiorze danych, przysługuje prawo kontroli treści ich danych osobowych, a szczególności prawo do uzyskania wyczerpujących informacji na temat tych danych, w każdym procesie przetwarzania danych w komórkach organizacyjnych Akademii Sztuk Pięknych w Gdańsku.
2. Każda osoba, która wystąpi z wnioskiem o otrzymanie informacji, otrzymuje odpowiedź na piśmie w terminie nie przekraczającym 30 dni od daty wpłynięcia wniosku, w formie pisemnej. Zakres odpowiedzi opracowuje Kierownik komórki merytorycznie odpowiedzialnej za przetwarzanie danych.
3. W przypadku gdy dane osoby są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy o ochronie danych osobowych, albo są zbędne do realizacji celu, dla którego zostały zebrane, użytkownik przetwarzający merytorycznie dane osobowe jest zobowiązany do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia w zakresie uzgodnionym z Administratorem Bezpieczeństwa Informacji.

Rozdział V

Ochrona przetwarzania zbiorów danych osobowych

§1

Akademia Sztuk Pięknych w Gdańsku jako ADO przestrzega zasad i przepisów oraz środków organizacyjnych i technicznych, zapewniających ochronę przetwarzanych danych, w szczególności przed ich udostępnianiem, kradzieżą, uszkodzeniem lub zniszczeniem przez osoby nieupoważnione. Realizacja nadzoru określona jest zakresem zadań ABI i podmiotu realizującego zadania ASI.
Zabezpieczenia realizowane w Akademii Sztuk Pięknych w Gdańsku na bieżąco monitoruje ABI.

§2

W celu realizacji powierzonych zadań Administrator Bezpieczeństwa Informacji ma prawo działać zgodnie z zakresem praw i obowiązków określonych w załączniku nr 2.

Rozdział VI

Zasady udostępnienia i powierzania danych osobowych

§1

Akademia Sztuk Pięknych w Gdańsku udostępnia dane osobowe przetwarzane we własnych zbiorach / w zbiorach powierzanych, wyłącznie osobom lub podmiotom uprawnionym do ich otrzymania z mocy przepisów prawa lub treścią paragrafu 2.

§2

1. Zbiory danych udostępnia się na pisemny wniosek, chyba że przepisy prawa stanowią inaczej w trybie art. 23 lub 27 UODO.
2. Wniosek jest rozpatrywany przez Administratora Danych Osobowych.
3. Decyzję w sprawie udostępnienia podejmuje Administrator Danych Osobowych osobiście lub upoważniona przez ADO osoba.
4. Administrator Danych Osobowych Akademia Sztuk Pięknych w Gdańsku, może odmówić udostępnienia danych osobowych, jeżeli spowodowałoby to istotne naruszenia dóbr osobistych osób, których dane dotyczą lub innych osób.

§3

1. Akademia Sztuk Pięknych w Gdańsku jako administrator danych może przetwarzanie danych osobowych powierzyć innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej – wzór umowy stanowi załącznik nr 1 do PBI.
2. Podmiot, o którym mowa w ust. 1 zobowiązany jest do zastosowania środków organizacyjnych i technicznych zabezpieczających zbiór przed dostępem osób nieupoważnionych na zasadach określonych w przepisach o ochronie danych osobowych oraz przepisach wykonawczych.
3. Za odpowiednią realizację powierzenia danych, [opracowanie projektu specyfikacji istotnych warunków zamówienia, projekt umowy], odpowiadają kierownicy komórek organizacyjnych w porozumieniu z ABI, a w zakresie spraw dotyczących informatyki ASI.

Część Druga

INSTRUKCJA POSTĘPOWANIA W SYTUACJACH NARUSZENIA OCHRONY DANYCH OSOBOWYCH

W OPARCIU O NORMĘ PN-ISO/IEC 17799:200727001:2007

§1

Celem instrukcji jest określenie sposobu postępowania Administratora Bezpieczeństwa Informacji w przypadku, gdy:

a) Stwierdzono naruszenie zabezpieczenia systemu informatycznego w obszarze przetwarzania danych osobowych Akademii Sztuk Pięknych w Gdańsku;
b) Stan urządzenia lub urządzeń w tym mobilnych, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci komputerowej mogą wskazywać na naruszenie przyjętych zasad bezpieczeństwa danych osobowych.

§2

Instrukcja określa zasady postępowania wszystkich osób zaangażowanych w procesach przetwarzania danych osobowych w systemach informatycznych lub nieinformatycznych.

§3

Naruszeniem zabezpieczenia systemu informatycznego, przetwarzającego dane osobowe jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia lub jakiegokolwiek elementu systemu informatycznego, a w szczególności:

a) nieautoryzowany dostęp do danych;
b) instalowanie nieautoryzowanych aplikacji lub programów;
c) nieautoryzowane modyfikacje lub zniszczenie danych;
d) udostępnienie danych nieautoryzowanym podmiotom;
e) nielegalne ujawnienie danych;
f) pozyskiwanie danych z nielegalnych źródeł.

§4

W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy użytkownik zaangażowany w procesie przetwarzania danych osobowych jest zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie powiadomić o tym fakcie bezpośredniego przełożonego lub ABI (ewentualnie osobę przez niego upoważnioną), a następnie postępować stosownie do podjętej przez niego decyzji.

Zgłoszenie naruszenia ochrony danych osobowych powinno zawierać:

a) opisanie symptomów naruszenia ochrony danych osobowych;
b) określenie sytuacji i czasu w jakim stwierdzono naruszenie ochrony danych osobowych;
c) określenie wszelkich istotnych informacji mogących wskazywać na przyczynę naruszenia;
d) informacje o prawdopodobnym zagrożeniu.

§5

Administrator Bezpieczeństwa Informacji lub inna upoważniona przez niego osoba podejmuje wszelkie działania mające na celu:

a) minimalizację negatywnych skutków zdarzenia;
b) wyjaśnienie okoliczności zdarzenia;
c) zabezpieczenie dowodów zdarzenia;
d) umożliwienie dalszego bezpiecznego przetwarzania danych.

§6

W celu realizacji zadań niniejszej Instrukcji Administrator Bezpieczeństwa Informacji Akademii Sztuk Pięknych w Gdańsku lub inna upoważniona przez niego osoba ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, a w szczególności:

a) żądania wyjaśnień od pracowników;
b) korzystania z pomocy konsultantów;
c) zawieszenie lub odebranie uprawnień do przetwarzania danych każdemu użytkownikowi;
d) nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.

§7

Polecenie Administratora Bezpieczeństwa Informacji wydawane w czasie realizacji zadań wynikających z niniejszej instrukcji są priorytetowe i winny być wykonywane przed innymi zapewniając ochronę danych osobowych w Akademii Sztuk Pięknych w Gdańsku.

§8

Odmowa udzielenia wyjaśnień lub współpracy z Administratorem Bezpieczeństwa Informacji traktowana będzie jako naruszenie obowiązków pracowniczych**.**

§9

1. Administrator Bezpieczeństwa Informacji po zażegnaniu sytuacji nadzwyczajnej opracowuje raport końcowy, w którym przedstawia przyczyny i skutki zdarzenia oraz wnioski, a także zasady ograniczające możliwość wystąpienia zdarzenia w przyszłości.

2. Wnioski kadrowe podejmuje według właściwości Rektor Uczelni.

§10

Nieprzestrzeganie zasad postępowania określonych w niniejszej instrukcji stanowi naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności dyscyplinarnej określonej w Kodeksie Pracy.

§11

Jeżeli skutkiem działania określonego w §10 jest ujawnienie informacji osobie nieupoważnionej, sprawca może zostać pociągnięty do odpowiedzialności karnej wynikającej z przepisów Kodeksu Karnego.

§12

Jeżeli skutkiem działania określonego w §10 jest szkoda, sprawca ponosi odpowiedzialność materialną na warunkach określonych w przepisach Kodeksu Pracy oraz Kodeksu Cywilnego.

§13

1. Ustala się następujący katalog zdarzeń stanowiących naruszenie ochrony danych osobowych:
   a) Zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu)- ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych;
   b) Zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania)- może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych;
   c) Zagrożenia zamierzone, świadome i celowe- najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy).
2. Zagrożenia te możemy podzielić na:
   a) nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu);
   b) nieuprawniony dostęp do system z wewnątrz;
   c) nieuprawniony przekaz danych.

W przypadku naruszenia systemu ochrony danych osobowych w Uczelni, każdy pracownik zobowiązany jest do stosowania zapisów postanowień INSTRUKCJI POSTĘPOWANIA W SYTUACJACH NARUSZENIA OCHRONY DANYCH OSOBOWYCH.

Część Trzecia

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

W OPARCIU O NORMĘ PN-ISO/IEC 17799:2007

Wprowadzenie

Instrukcja Zarządzania Systemem Informatycznym **Akademii Sztuk Pięknych** w Gdańsku, zwana dalej „instrukcją" określa sposób zarządzania systemem informatycznym służącym do przetwarzania danych. Określony w instrukcji sposób zarządzania systemem informatycznym zapewnia jednolity sposób postępowania przy przetwarzaniu danych osobowych. Naruszenie przez użytkownika niniejszej instrukcji może zostać potraktowane jako naruszenie obowiązków pracowniczych i powodować określoną przepisami kodeksu pracy odpowiedzialność pracownika. W sprawach nie uregulowanych w niniejszej instrukcji mają zastosowanie przepisy o ochronie danych osobowych i inne akty prawne wydane na ich podstawie.

1.Procedura nadawania uprawnień do przetwarzania danych

Do przetwarzania danych osobowych i obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład dopuszcza się wyłącznie osoby posiadające upoważnienie wydane przez ADO lub osobę przez niego upoważnioną. Osobą odpowiedzialną za administrowanie systemem informatycznym jest ASI, który posiada upoważnienie do obsługi użytkownika we wszystkich systemach informatycznych Uczelni. ASI może wystąpić o nadanie statusu uprzywilejowanego użytkownika, dla osoby pełniącej funkcję Administratora Systemu Informatycznego.

2.Upoważnienia i uprawnienia do przetwarzania danych

Upoważnienia użytkownikom przetwarzającym dane osobowe podpisuje Rektor lub osoba upoważniona na wniosek ABI i kierownika komórki organizacyjnej. Upoważnienia kierownikom komórek organizacyjnych oraz ich wycofanie wydaje ADO, na wniosek przełożonego sprawującego nad nimi bezpośredni nadzór. Kierownik komórki organizacyjnej zobowiązany jest do złożenia wniosku o udzielenie upoważnienia do przetwarzania danych osobowych dla osób podległych, które będą przetwarzały dane osobowe zgodnie ze wzorem wniosku określonym w załączniku nr 3 niniejszej instrukcji. Wniosek składany jest do Rektora, za pośrednictwem ABI, który przygotuje treść upoważnienia zgodnie z wzorem upoważnienia określonym w załączniku nr 4 niniejszej instrukcji. Jeżeli wniosek o udzielenie upoważnienia dot. zbioru danych osobowych utworzonego w innej komórce organizacyjnej wymagana jest akceptacja na wniosku kierownika komórki organizacyjnej. Dokument upoważnienia przechowywany jest przez ABI w specjalnie do tego celu utworzonym rejestrze. Informacja dotycząca udzielenia upoważnienia przekazywana jest ASI. Cofnięcie upoważnienia następuje na wniosek kierownika komórki organizacyjnej, w której użytkownik przetwarzał dane osobowe, zgodnie ze wzorem wniosku o cofnięcie upoważnienia określonym w załączniku nr 5 niniejszej instrukcji. Wniosek składny jest ADO, za pośrednictwem ABI, który przygotowuje treść cofnięcia upoważnienia zgodnie z wzorem cofnięcia upoważnienia określonym w załączniku nr 6 niniejszej instrukcji. Informacja dotycząca cofnięcia upoważnienia przekazywana jest

ASI, który usuwa pracownikowi odpowiednie uprawnienia w systemie informatycznym, w którym były przetwarzane dane osobowe.

3.Zasady przydzielania identyfikatorów (loginów)

Dla każdego użytkownika systemu informatycznego ustala się odrębny identyfikator, który rejestruje się w rejestrze przydzielonych identyfikatorów. Dostęp oraz identyfikator do systemów informatycznych przydzielany jest przez ASI na wniosek kierownika komórki organizacyjnej zgodnie z wzorem wniosku określonym załączniku nr 7 niniejszej instrukcji. ASI rejestruje wszystkie zmiany w zakresie nadawania i cofania uprawnień w systemach informatycznych w rejestrze przydzielonych identyfikatorów. Rejestr przydzielonych identyfikatorów powinien zawierać m.in. imię i nazwisko, identyfikator użytkownika, zakres dostępu, nazwę programu, datę udzielenia dostępu, datę utraty ważności identyfikatora. W celu jednoznacznego określenia użytkowników przyjmuje się następującą metodologię nadawania nazw kont:

a) pierwsza litera imienia i nazwisko lub imię.nazwisko

przykład: **Jan Kowalski**, identyfikator (login): **jkowalski, lub jan.kowalski**

W tworzeniu identyfikatora stosuję się litery alfabetu łacińskiego i cyfry arabskie. Powyższe zasady nie dotyczą systemów informatycznych, w których nazwa użytkownika jest tworzona przez sam system. Jeżeli nowo tworzony identyfikator byłby zbieżny z już istniejącym, do identyfikatora dodaje się cyfrę (np. jkowalski1 lub jan.kowalski1).

Cofnięcie dostępu oraz unieważnienie identyfikatora do systemów informatycznych realizowane jest przez ASI na wniosek kierownika komórki organizacyjnej zgodnie z wzorem wniosku określonym w załączniku nr 8 niniejszej instrukcji. Identyfikator, który utracił ważność nie może być przydzielany innemu użytkownikowi.

4.Konstruowanie haseł

Do uwierzytelniania użytkowników w systemach informatycznych używa się hasła składającego się z co najmniej 8 znaków, zawierającego małe i wielkie litery oraz cyfry i znaki specjalne. Przydział hasła polega na umożliwieniu użytkownikowi wpisania w systemie informatycznym hasła, którym będzie się posługiwał. Zmiana hasła następuję nie rzadziej co 30 dni. Jeżeli system informatyczny nie wymusza zmiany hasła, użytkownik jest zobowiązany pamiętać o jego zmianie. W przypadku, gdy użytkownik zapomni hasła, zwraca się o ponowny jego przydział. Osobą odpowiedzialną za przydzielenie haseł jest ASI.

5.Przechowywanie haseł

Zabrania się udostępniania haseł przez użytkowników w jakiejkolwiek formie osobom postronnym. Hasła użytkowników, umożliwiające dostęp do systemu informatycznego utrzymuje się w tajemnicy, również po upływie ich ważności. Hasła użytkowników, będącymi administratorami w systemach informatycznych tzw. „admin", przechowuje się w postaci papierowej w stosownie zabezpieczonym miejscu.

6.Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

Przed przystąpieniem do przetwarzania danych osobowych w systemie informatycznym użytkownik tego systemu powinien sprawdzić czy nie nastąpiło naruszenie środków ochrony danych osobowych. W przypadku stwierdzenia naruszenia środków ochrony danych osobowych należy niezwłocznie powiadomić

o tym fakcie ABI. Za naruszenie środków ochrony danych osobowych uważa się sytuację gdy:

a) stwierdzono naruszenie fizyczne zabezpieczeń pomieszczeń, budynków stanowiących obszar w którym przetwarzane są dane osobowe;
b) stan urządzenia, zawartość zbioru danych osobowych, sposób działania programu wskazują na naruszenie danych osobowych;
c) ujawnione zostały metody pracy osobom nie posiadającym upoważnienia do przetwarzania danych, a w szczególności ujawniono system haseł umożliwiający dostęp do systemów informatycznych;
d) nośniki informacji i wydruki z danymi osobowymi nie są przechowywane w warunkach uniemożliwiających dostęp do nich osobom nieupoważnionym.

Użytkownik loguje się do systemu operacyjnego oraz uruchamia systemy informatyczne służące do przetwarzania danych osobowych używając do tego celu własnej nazwy użytkownika i własnego hasła dostępu. W czasie dłuższych przerw w pracy, użytkownik zabezpiecza możliwość wglądu w wyświetlane na monitorze dane przez osoby nieupoważnione, wykonując czynności związane z zakończeniem przetwarzania danych osobowych w systemie informatycznym. Po zakończeniu przetwarzania danych osobowych w systemie informatycznym, należy opuścić system użytkowy i sieciowy system operacyjny, dokonując wylogowania z systemu (zamknięcia systemu), wyłączyć komputer, a jeżeli zakończenie przetwarzania danych osobowych związane jest z opuszczeniem pomieszczenia przez wszystkie osoby przetwarzające dane osobowe w danym pomieszczeniu, należy zabezpieczyć pomieszczenie przed dostępem do niego osób nieupoważnionych.

7.Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

Za wszystkie czynności związane z tworzeniem kopii zapasowych, ich testowaniem, przechowywaniem oraz likwidacją nośników odpowiedzialny jest ASI. Należy przeprowadzać okresowe archiwizacje kopi zapasowych jako główne zabezpieczenia danych przed utratą. W celu usprawnienia procesu archiwizacji baz danych, systemy informatyczne służące do przetwarzania danych osobowych należy instalować na serwerze.

8.Metody i częstotliwość tworzenia kopii

W systemach informatycznych, które opierają się o pracę w technologii klient-serwer kopie zapasowe wykonuje się po stronie serwera. Dla indywidualnych systemów informatycznych pracujących na pojedynczych komputerach, lub w małym otoczeniu sieciowym, kopie zapasowe wykonuje się na komputerze, na którym zainstalowany jest dany program, a także na serwerze. W takim przypadku ASI wyznacza osobę, która odpowiedzialna jest za wykonywanie kopii zapasowej. Częstotliwość wykonywania kopii zapasowych uzależniona jest od specyfiki danego stanowiska pracy oraz od ilości przechowywanych danych, systemy przechowujące wrażliwe dane objęte są wykonywaniem kopii zapasowych nie rzadziej niż raz na 7 dni, pozostałe nie rzadziej niż raz na 30 dni. Zabezpieczone dane przechowywane są na serwerze kopii zapasowej. Niedopuszczalne jest przechowywanie pojedynczej kopii zapasowej wyłącznie na tym samym komputerze, w którym pracuje lub jest zainstalowane oprogramowanie. Wszystkie wykonane kopie zapasowe zapisuje się na nośnikach.

9.Wykonywanie archiwizacji i ich przechowywanie

Archiwizacje wykonuje się jako kopie całościowe baz danych. Okres przechowywania zarchiwizowanej kopii wynosi jeden rok licząc od dnia jej wykonania. Po upływie okresu przechowywania i ocenie wartości, zbędne kopie przeznacza się do likwidacji.

10.Elektroniczne nośniki informacji zawierające dane osobowe

Dane osobowe przechowuje się na dyskach twardych komputerów lub dyskach serwerów w zależności od zastosowanego systemu. Stacje robocze, na których są przechowywane dane osobowe wyznaczają kierownicy komórek organizacyjnych w uzgodnieniu z ASI. W przypadku serwerów ich ochrona polega na wyizolowaniu urządzeń w odrębnych zamykanych pomieszczeniach, do których dostęp posiadają wyłącznie ADO, ABI, ASI, pracownicy serwisu konserwacyjnego oraz inne upoważnione przez ABI osoby. Zabrania się wynoszenia poza obszar przetwarzania danych wszelkich nośników zawierających dane osobowe typu płyty CD, DVD, dyski twarde (HDD), pendrive, RDX, macierze dyskowe. Zakaz wynoszenia poza obszar przetwarzania danych dotyczy także przenośnego sprzętu komputerowego typu notebook, palmtop, itp. z wyłączeniem osób upoważnionych przez ADO.

11.Likwidacja nośników zawierających dane osobowe

W przypadku nośników jednorazowych takich jak płyty CD-R, DVD-R likwidacja polega na ich fizycznym zniszczeniu, w sposób, uniemożliwiający odczytanie ich zawartości, np. niszczarki płyt CD. Nośniki wielorazowego użytku takie jak dyski twarde (HDD), dyskietki, płyty CD-RW, DVD-RW, itp. można wykorzystać ponownie do celów przechowywania kopii zapasowych po uprzednim usunięciu ich zawartości. Nośniki wielorazowego użytku nie nadające się do ponownego użycia zniszczone są fizycznie w sposób trwały.

12.Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu

do systemu informatycznego Akademii Sztuk Pięknych w Gdańsku, zalicza się sprzęt komputerowy (komputer, monitor, klawiatura, mysz, drukarka, skaner oraz pozostałe urządzenia peryferyjne wchodzące w skład sprzętu komputerowego); oprogramowanie komputerowe (system operacyjny, pakiet aplikacji biurowej, oprogramowanie antywirusowe oraz inne oprogramowanie użytkowe); zewnętrzne nośniki danych (taśmy, dyskietki, płyty CD i DVD typu R i RW, itp.); Internet (strony WWW, poczta elektroniczna, usługi typu ftp, telnet, itp.). System informatyczny używany jest wyłącznie do celów służbowych. Dopuszcza się możliwość zakupu oprogramowania komputerowego przez inne komórki organizacyjne w ramach posiadanych własnych środków budżetowych. Wymagana jest jednoczesna akceptacja ASI potwierdzająca zgodność sprzętową i systemową zakupywanego oprogramowania komputerowego z istniejącym sprzętem komputerowym. Zgłoszenia zapotrzebowania instalacji lub udostępnienia oprogramowania komputerowego na danym stanowisku komputerowym dokonują kierownicy komórek organizacyjnych bezpośrednio ASI. Zgłoszenia może dokonać zainteresowany pracownik jeśli zgłoszenie dotyczy oprogramowania z pakietu programów podstawowych. Listę programów wchodzących w skład pakietu programów podstawowych ustala ASI. Dopuszcza się instalowanie i używanie tylko oprogramowania komputerowego posiadającego licencję rozumianą jako zgoda autora oprogramowania na jego używanie, pozyskanego przez Akademię Sztuk Pięknych w Gdańsku. Zabrania się

instalowania i używania prywatnego oprogramowania komputerowego, nawet jeśli posiada ono odpowiednią legalną licencję.

13.Obszary systemu informatycznego narażone na ingerencję wirusów komputerowych oraz innego oprogramowania

Na działanie wirusów komputerowych narażone są wszystkie stanowiska komputerowe, które są przyłączone do sieci komputerowej oraz te, które są wyposażone w czytniki nośników elektronicznych takich jak czytniki optyczne i inne nośniki danych umożliwiające wprowadzenie danych lub programów z zewnątrz.

14.Źródła przedostawania się szkodliwego oprogramowania do systemów

Do źródeł szkodliwego oprogramowania m.in. można zaliczyć pliki zapisane na nośnikach elektronicznych, pliki przesyłane za pomocą poczty elektronicznej, pliki pobierane ze stron internetowych, pliki prywatne użytkowników. Czynności nadzorcze wykonuje ASI Akademii Sztuk Pięknych w Gdańsku.

15.Czynności profilaktyczne minimalizujące wpływ szkodliwego oprogramowania ASI zobowiązany jest, do wprowadzenia sprzętowych i programowych zabezpieczeń blokujących działanie niepożądanego oprogramowania w systemie oraz szkolenia w zakresie bezpiecznego użytkowania systemu informatycznego dla osób rozpoczynających pracę na stanowisku komputerowym. Systemy informatyczne, w których przetwarzane są dane osobowe, należy okresowo sprawdzać pod kątem obecności wirusów komputerowych. Sprawdzenia obecności i usuwanie wirusów dokonuje się za pomocą dostępnych programów antywirusowych. Sprawdzenia obecności wirusów komputerowych należy przeprowadzać co najmniej dwa razy w roku oraz każdorazowo w przypadku domniemanego ich występowania. Wszystkie stanowiska komputerowe wyposażone są w indywidualną ochronę antywirusową. Użytkownik przed użyciem zewnętrznego nośnika danych powinien sprawdzić go programem antywirusowym. Po wykryciu wirusa na stanowisku komputerowym lub zewnętrznym nośniku danych należy zaprzestać ich użytkowania oraz powiadomić ASI.

16.Spełnienie wymogu rejestracji czynności wykonywanych przez użytkowników podczas ewidencji i przetwarzania danych osobowych w systemach informatycznych

Wszystkie systemy informatyczne, służące do ewidencji i przetwarzania danych osobowych powinny zawierać mechanizmy rejestracji wprowadzanych zmian oraz rejestracji udostępnianych danych. Informacje o zmianach i o udostępnieniach danych są odnotowywane w sposób elektroniczny poprzez automatyczne zapisy w bazach danych systemów z uwzględnieniem identyfikatora osoby, daty a także wykonywanej czynności. Odnotowanie obejmuje informacje o nazwie podmiotu lub imieniu i nazwisku osoby, której udostępniono dane, zakresie udostępnienia danych, dacie udostępnienia. Obowiązek odnotowania w/w informacji spoczywa na użytkowniku systemu, w tym celu wypełnia on odpowiednie pole w bazie danych osobowych, arkuszu kalkulacyjnym lub tabeli w edytorze tekstu. Odnotowanie informacji powinno nastąpić niezwłocznie po udostępnieniu danych.

17.Cele wykonywania przeglądów, konserwacji i napraw

Wykonywanie przeglądów, konserwacji i napraw ma na celu zapewnienie ciągłości pracy systemów informatycznych w Akademii Sztuk Pięknych w Gdańsku, poprzez eliminowanie niespodziewanych awarii wskutek naturalnego zużycia się urządzeń, wykrywanie i eliminacja ewentualnych zagrożeń wynikających z pracy systemów bez

okresowej kontroli (np. uszkodzone elementy chłodzenia systemów), dostrzeganie potrzeb modyfikacji istniejącej infrastruktury, wykrywanie niesprawnych nośników powodujących problemy lub wprowadzających przekłamania przy przenoszeniu danych.

18.Zakres wykonywanych przeglądów, konserwacji i napraw

Przeglądu i konserwacji wszystkich systemów informatycznych oraz nośników informacji dokonuje ASI lub pracownicy firm posiadających prawa autorskie do systemów, po uzyskaniu zgody ASI. W przypadku zlecenia wykonania powyższych czynności podmiotowi zewnętrznemu, wszelkie prace powinny przebiegać pod nadzorem ASI. Po dokonaniu zmian funkcjonalnych w systemie informatycznym należy sprawdzić poprawność rejestrowania się w systemie oraz poprawność działania poszczególnych elementów aplikacji. Przeglądu i kontroli poprawności danych osobowych dokonują na bieżąco osoby upoważnione do przetwarzania danych w czasie pracy z danymi osobowymi. Komputery, drukarki, skanery, monitory, dyski twarde, napędy optyczne, elementy elektroniczne, a także inny sprzęt peryferyjny poddawany jest jedynie ogólnym przeglądom. Czynności serwisowe wykonywane są przez:

a) specjalistyczne punkty serwisowe w przypadku kiedy systemy informatyczne: objęte są gwarancją,- nie objęte są gwarancją, ale specyfika przeglądu, konserwacji tego wymaga;
b) ASI w przypadku kiedy systemy informatyczne: nie objęte są gwarancją, - objęte są gwarancją, ale przegląd, konserwacja nie narusza warunków gwarancji.

19.Bezpieczeństwo nośników przekazywanych do naprawy

Nośniki, które uległy uszkodzeniu, zawierające dane osobowe można przekazać do naprawy pod warunkiem, że firma posiada autoryzację i wystawi stosowne oświadczenie, o zapewnieniu poufności ewentualnie pozyskanych informacji. W przypadku przekazywania całego urządzenia (stacji roboczej) do naprawy należy zadbać o to, aby przed przekazaniem urządzenia pozbawić go nośników zawierających dane lub jeśli jest to nie możliwe usunąć te dane z nośnika w sposób uniemożliwiający ich odzyskanie. W sytuacji gdy nie ma możliwości usunięcia danych, dopuszcza się naprawę urządzenia w obecności osoby upoważnionej przez ADO.

20.Postępowanie w sytuacji naruszenia ochrony danych osobowych

Za naruszenie ochrony danych osobowych uznaje się przypadki, w których stwierdzono naruszenie zabezpieczenia systemu teleinformatycznego, a także kiedy stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci teleinformatycznej mogą wskazywać na naruszenie zabezpieczeń tych danych.

Każdy użytkownik, który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych w systemie teleinformatycznym zobowiązany jest do niezwłocznego poinformowania o tym ABI. Po przywróceniu pierwotnego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyn naruszenia ochrony danych osobowych. Po przygotowaniu szczegółowego raportu o przyczynach, przebiegu i wnioskach ze zdarzenia ABI przedstawia go ADO wraz z propozycjami podjęcia odpowiednich działań mających na celu zapobieżenie w przyszłości podobnym zdarzeniom.

Umowa powierzenia danych

zabezpieczenie powierzonych danych osobowych

1. Wykonawca zobowiązuje się do ochrony danych, zgodnie z ustawą o ochronie danych osobowych, oraz zgodnie z powszechnie przyjętymi standardami i ustalonymi przez Strony warunkami. Obowiązek zachowania tajemnicy obejmuje wszystkich uczestników procesu realizacji umowy w szczególności wszelkie informacje, dane, materiały uzyskane w związku z zawarciem Umowy.
2. Akademia Sztuk Pięknych w Gdańsku jest administratorem danych osobowych w rozumieniu przepisów ustawy z dnia 29 sierpnia 1997 (Dz.U.02.101.926 z póź. zm) o ochronie danych osobowych zwanej dalej „Ustawą", jednocześnie w pełni realizuje odpowiednią ochronę danych zgodnie z dyspozycją art. 36-39 Ustawy.
3. Zamawiający powierza a Wykonawca zobowiązuje się przetwarzać powierzone mu na podstawie art. 31 Ustawy dane osobowe wyłącznie w zakresie oraz celu związanym z realizacją postanowień niniejszej Umowy na dostarczanie usług. Przetwarzanie przez Wykonawcę danych osobowych w zakresie oraz celach innych niż wyraźnie wskazane powyższymi postanowieniami oraz objęte upoważnieniem udzielanym w treści niniejszej Umowy jest niedopuszczalne.
4. Dane osobowe stanowiące zbiór danych udostępniane Wykonawcy w warunkach niniejszego paragrafu, zawierają się w następującym zakresie:
   a) nazwiska; imienia; nr PESEL
   b) inne dane…….
5. Wykonawca zobowiązuje się do zastosowania przy przetwarzaniu danych osobowych, środków technicznych i organizacyjnych zapewniających ochronę danych, w zakresie określonym w art. 36-39a Ustawy, przedkładając Zamawiającemu oświadczenie wykazujące stosowanie właściwych środków zabezpieczenia danych osobowych (PBI). Wykonawca jest obowiązany zapewnić, aby urządzenia i systemy informatyczne służące do przetwarzania powierzonych danych osobowych były zgodne z wymogami 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).
6. Wykonawca oraz Zamawiający oświadczają, że do pełnienia funkcji administratorów bezpieczeństwa informacji wyznaczono następujące osoby: 1…… 2……
7. Wykonawca zobowiązuje się przesłać Zamawiającemu imienne upoważnienia (kopie) osób, które będą przetwarzały dane osobowe zgodnie z postanowieniami niniejszej Umowy.
8. W przypadku wygaśnięcia niniejszej Umowy, Wykonawca jest bezwzględnie zobowiązany do *usunięcia* (zwrotu lub zniszczenia potwierdzonego protokółem, powierzonych mu danych osobowych) oraz skasowania wszelkich kopii tych danych będących w posiadaniu Wykonawcy oraz podjąć działania w celu wyeliminowania możliwości dalszego przetwarzania danych powierzonych na podstawie niniejszej Umowy.

Zakres praw i obowiązków Administratora Bezpieczeństwa Informacji oraz Administratora Systemu Informatycznego

1. Administrator Bezpieczeństwa Informacji odpowiada za bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych oraz w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych Akademii Sztuk Pięknych w Gdańsku, w zakresie zgodności zasad postępowania przy przetwarzaniu danych z obowiązującymi przepisami o ochronie danych osobowych.
2. Do zadań Administratora Bezpieczeństwa Informacji należy w szczególności:
   a) nadzór nad zasadami zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe oraz kontrolą przebywających w nich osób;
   b) nadzór merytoryczny nad prowadzeniem ewidencji wydanych upoważnień i oświadczeń;
   c) nadzór nad przechowywaniem kopii zapasowych poprzez ewidencje prowadzoną przez ASI;
   d) nadzór i kontrola ASI, oraz pozostałych użytkowników upoważnionych do przetwarzania danych osobowych;
   e) organizacja zajęć szkoleniowych pracowników Uczelni, po zmianach przepisów Ustawy o ochronie danych osobowych; szkolenie instruktażowe pracowników z zakresu ochrony danych osobowych prowadzą Kierownicy komórek merytorycznych.
3. Do zadań Administratora Systemu Informatycznego należy:
   a) nadzór nad uprawnieniami użytkowników, w procesach przetwarzania danych w systemie informatycznym Uczelni;
   b) zarządzanie hasłami użytkowników i nadzór nad przestrzeganiem procedur określających częstotliwość ich zmiany;
   c) nadzór nad czynnościami związanymi z zarządzaniem systemami w zakresie:
      - obecności wirusów;
      - częstości ich sprawdzania oraz nadzorowanie wykonywanych procedur uaktualnienia systemów antywirusowych i ich konfiguracji;
      - rejestru nośników służbowych;
   d) wykonywanie kopii zapasowych systemu informatycznego, weryfikacja przydatności kopii a także likwidacja nośników;
   e) nadzór nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących do przetwarzania danych osobowych;
   f) zapewnienie bezawaryjnego działania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych;
   g) zapewnienie ciągłości działania systemu informatycznego.
4. Lokalny Administrator Bezpieczeństwa Informacji- Kierownicy działów merytorycznych realizują w zakresie ochrony danych osobowych przede wszystkim następujące zadania:
   a) występują z wnioskiem do administratora danych o nadanie pracownikom / użytkownikom, stażystom upoważnienia do przetwarzania danych osobowych;

b) występują z wnioskiem do administratora systemu sieci /ASI/ o nadanie identyfikatora i przyznanie hasła osobie upoważnionej do przetwarzania danych osobowych;
c) występują z wnioskiem o:
    - odwołanie upoważnienia do przetwarzania danych osobowych;
    - zmianę uprawnień w systemie;
    - wyrejestrowania użytkownika z systemu informatycznego.
d) użytkownik ma obowiązek należycie zabezpieczyć przyznane dane logowania.

Załącznik nr 3 do Polityki bezpieczeństwa informacji
Akademii Sztuk Pięknych w Gdańsku

Wniosek o wydanie upoważnienia

Wnioskuję o wydanie upoważnienia

dla Pana/Pani …..……..……..……..…….. …..…….……..…….
Imię i Nazwisko Stanowisko

w ……..……..……..……..…….
nazwa jednostki organizacyjnej

do przetwarzania danych osobowych zawartych w:

……w zakresie: **edycja danych/podgląd danych lub inny zakres***
nazwa ZDO

…….. ……..……..……..……..……..…..…
data wniosku podpis bezpośredniego przełożonego/akceptacja właściciela zbioru
(w przypadku zbioru w innej komórce organizacyjnej)

……..……..……..…….
akceptacja administratora danych

Załącznik nr 4 do Polityki bezpieczeństwa informacji
Akademii Sztuk Pięknych w Gdańsku

Upoważnienie

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 ze zm.) upoważniam

dla Pana/Pani …..……..……..……..……..… …..…….……..……..
Imię i Nazwisko Stanowisko

w ……..……..……..……..…….
nazwa jednostki organizacyjnej

do przetwarzania danych osobowych zawartych w:

……**w zakresie: edycja danych/podgląd danych/ inne***
nazwa ZDO

……..……..…… ……..……
data nadania upoważnienia podpis administratora danych

Otrzymują:
- upoważniony;
- ABI;
- ASI;
- a/a.

* niepotrzebne skreślić

Załącznik nr 5 do Polityki bezpieczeństwa informacji
Akademii Sztuk Pięknych w Gdańsku

Wniosek o cofnięcie upoważnienia

Wnioskuję o cofnięcie upoważnienia

dla Pana/Pani …..……..……..……..…….. …..……..…….
Imię i Nazwisko Stanowisko

w ……..……..……..……..……
nazwa jednostki organizacyjnej

do przetwarzania danych osobowych zawartych w:

……w zakresie: **edycja danych/podgląd danych lub inny zakres***
nazwa ZDO

…….. ……..……..……..……..……..…..
data wniosku podpis bezpośredniego przełożonego/akceptacja właściciela zbioru
(w przypadku zbioru w innej komórce organizacyjnej)

……..……..……..
akceptacja administratora danych

Załącznik nr 6 do Polityki bezpieczeństwa informacji
Akademii Sztuk Pięknych w Gdańsku

Informacja o cofnięciu upoważnienia

Cofam upoważnienie

dla Pana/Pani …..……..……..……..…….. …..……..…….
Imię i Nazwisko Stanowisko

w ……..……..……..……..……
nazwa jednostki organizacyjnej

do przetwarzania danych osobowych zawartych w:

……**w zakresie: edycja danych/podgląd danych/ inne***
nazwa ZDO

……..…… ……
data cofnięcia upoważnienia podpis administratora danych

Otrzymują:
- Adresat;
- ABI;
- ASI;
- a/a.

* niepotrzebne skreślić

Załącznik nr 7 do Polityki bezpieczeństwa informacji w Akademii Sztuk Pięknych w Gdańsku

Wniosek o przydzielenie dostępu

Wnioskuję o przydzielenie identyfikatora/dostępu

dla Pana/Pani …..…….…..……..……..…….. …..…….…..……..
Imię i Nazwisko Stanowisko

w ……..…….…..……..……..
nazwa jednostki organizacyjnej

do programu/systemu informatycznego: ……..……..
nazwa systemu informatycznego

w zakresie: edycja danych/podgląd danych/ inne*

……..……..…… ……..……..
data wniosku podpis bezpośredniego przełożonego

Przydzielono identyfikator/dostęp: ……..

……..……..…… ……..……..
data przydzielenia podpis przydzielającego

Załącznik nr 8 do Polityki bezpieczeństwa informacji Akademii Sztuk Pięknych w Gdańsku

Wniosek o cofnięcie dostępu

Wnioskuję o unieważnienie identyfikatora/cofnięcie dostępu

dla Pana/Pani …..…….…..……..……..…….. …..…….…..……..
Imię i Nazwisko Stanowisko

w ……..…….…..……..……..
nazwa jednostki organizacyjnej

do programu/systemu informatycznego: ……..……..
nazwa systemu informatycznego

w zakresie: edycja danych/podgląd danych/ inne*

……..……..…… ……..……..
data wniosku podpis bezpośredniego przełożonego

Unieważniono identyfikator/cofnięto dostęp: ……..

……..……..…… ……..……..
data cofnięcia podpis wykonującego

Załącznik nr 9 do Polityki bezpieczeństwa informacji
Akademii Sztuk Pięknych w Gdańsku

Wzór karty sprzętu komputerowego użytkownika

Nr inwentarzowy				
Użytkownik				
IP				
Nazwa programu	**nr licencji**	**typ programu**	**osoba instalująca**	**potwierdzenie instalacji przez użytkownika**