INSTRUKCJA
ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W AKADEMII SZTUK PIĘKNYCH IM. EUGENIUSZA GEPPERTA WE WROCŁAWIU

Zgodnie z Rozporządzeniem 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, Administrator Danych wdraża dokument o nazwie „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Akademii Sztuk Pięknych im. Eugeniusza Gepperta we Wrocławiu" zwanym dalej „instrukcją". Zapisy tego dokumentu wchodzą w życie z dniem podpisania zarządzenia, którego załącznikiem jest przedmiotowa instrukcja.

§ 1
PRZEDMIOT INSTRUKCJI

Instrukcja w szczególności określa zagadnienia związane z bezpieczeństwem danych gromadzonych, transmitowanych i przechowywanych w systemach informatycznych uczelni, a także sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji, w tym szczegółowe określenie:

a) poziomu bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym,
b) procedur nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym,
c) stosowanych metod i środków uwierzytelniania oraz procedur związanych z ich zarządzaniem i użytkowaniem,
d) sposobów przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz osób odpowiedzialnych za te czynności,
e) procedur rozpoczęcia, zawieszenia i zakończenia pracy przeznaczonych dla użytkowników systemu,
f) metod i częstotliwości tworzenia kopii zapasowych,
g) metod i częstotliwości sprawdzania obecności wirusów komputerowych oraz metod ich usuwania,
h) sposobu, miejsca i okresu przechowywania:
   - elektronicznych nośników informacji zawierających dane osobowe,
   - kopii archiwalnych,
i) sposobu dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych,
j) sposobu postępowania w zakresie komunikacji w sieci komputerowej,
k) procedur wykonywania przeglądów i konserwacji systemu oraz nośników informacji służących do przetwarzania danych.

§ 2
PROCEDURY NADAWANIA, MODYFIKACJI I ANULOWANIA UPRAWNIEŃ
DO PRZETWARZANIA DANYCH

1. Dostęp do systemu informatycznego Uczelni mogą posiadać:
   a) pracownicy – w zakresie niezbędnym do wykonywania powierzonych im czynności służbowych,
   b) wykonawcy usług oraz dostawcy sprzętu lub oprogramowania – w zakresie koniecznym do realizowania danej usługi lub wykonania określonych czynności w systemie.
2. Bezpośredni dostęp do danych osobowych jest możliwy wyłącznie przez osoby posiadające pisemne upoważnienie wydane przez Administratora Danych Osobowych (ADO) lub Lokalnych Administratorów Danych Osobowych (LADO), określające zakres dostępu do przetwarzanych danych zarówno w postaci tradycyjnej, jak i w systemie informatycznym.
3. Przy zatrudnianiu, Pracownik otrzymuje kartę obiegową.
4. W przypadku zakończenia stosunku pracy LADO usuwa dostęp do e- mail i następuje automatyczna blokada do kont.
5. W przypadku zapomnienia hasła, pracownik zgłasza ten fakt do Sekcji IT i generowane jest tzw. hasło jednorazowe/startowe.
6. Nadawanie uprawnień do systemów elektronicznych nadawane i odbierane jest przez wyznaczone osoby (administratorzy systemów dziedzinowych) na prośbę LADO.
7. Upoważnienia nadawane są do zbiorów na wniosek LADO. Upoważnienia określają zakres operacji na danych.
8. Wzór upoważnienia stanowi **załącznik nr 5** do Polityki Bezpieczeństwa.
9. Zakres przetwarzania danych osobowych jest adekwatny do zakresu zadań wykonywanych przez użytkownika, nie może być on szerszy, niż wynika to z realizowanych czynności zleconych przez LADO (lub osoby przez niego upoważnionej).
10. Zakres czynności realizowanych przez użytkownika systemu określa zakres jego dostępu do danych osobowych, odpowiedzialności za ich ochronę przed niepowołanym dostępem, nieuzasadnioną modyfikacją, zniszczeniem oraz ich nielegalnym ujawnieniem i pozyskaniem.
11. Użytkownik systemu zostanie dopuszczony do przetwarzania danych osobowych po odbyciu szkolenia oraz podpisaniu oświadczenia.
12. Wzór oświadczenia stanowi **załącznik nr 9** do Polityki Bezpieczeństwa.
13. W przypadku zmiany stanowiska lub zakresu obowiązków, jeśli jest to wymagane w celu umożliwienia prawidłowej realizacji zadań, powinna nastąpić modyfikacja uprawnień nadanych użytkownikowi.

14. Anulowanie praw dostępu użytkownika do danych osobowych następuje wraz z rozwiązaniem stosunku pracy lub w przypadku cofnięcia mu uprawnień na zlecenie jego przełożonego. LADO prowadzi „Ewidencję osób uprawnionych do przetwarzania danych osobowych". Ewidencja może być prowadzona w formie papierowej lub elektronicznej. Ewidencja prowadzona jest na podstawie nadanych/odebranych uprawnień do przetwarzania danych. Musi ona odzwierciedlać aktualny stan w zakresie użytkowników i ich uprawnień. Ewidencja osób upoważnionych do przetwarzania danych osobowych powinna zawierać:
    a) imię i nazwisko osoby upoważnionej oraz nazwę jednostki organizacyjnej, w której jest zatrudniona,
    b) datę nadania i ustania oraz zakres upoważnienia.

§ 3

REJESTROWANIE UPRAWNIEŃ DO PRZETWARZANIA DANYCH W SYSTEMIE INFORMATYCZNYM

1. Przyznanie uprawnień w zakresie dostępu do danych przetwarzanych w systemie informatycznym polega na wprowadzeniu do systemu, przez wyznaczone osoby (administratorzy systemów dziedzinowych), dla każdego użytkownika osobno, identyfikatora i hasła oraz zakresu dostępu do danych i operacji.
2. Ustanowione hasło dostępu administrator systemu dziedzinowego przekazuje użytkownikowi.
3. Każdy z użytkowników systemu posiada własne hasło i identyfikator.
4. Hasło ustanowione podczas przyznawania uprawnień należy zmienić na indywidualne podczas pierwszego logowania się w systemie informatycznym.
5. Użytkownik ma prawo do wykonywania w systemie tylko tych czynności, do których został upoważniony. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako naruszenie podstawowych obowiązków pracowniczych zagrożone karą dyscyplinarną.
6. Użytkownik ponosi odpowiedzialność za wszelkie operacje wykonywane przy użyciu jego identyfikatora i hasła.
7. W systemie informatycznym stosuje się uwierzytelnienie na poziomie dostępu do sieci lokalnej (w przypadku komputerów nie powiązanych z siecią – do systemu operacyjnego) oraz dostępu do aplikacji.
8. W przypadku anulowania uprawnień użytkownika jego identyfikator należy niezwłocznie zablokować w systemie informatycznym, w którym przetwarzane są dane osobowe oraz unieważnić hasło użytkownika.
9. Administrator Systemów Dziedzinowych prowadzi **„Rejestr użytkowników systemów"**, w którym odnotowuje imię i nazwisko, identyfikator, zakres uprawnień użytkownika oraz datę nadania, modyfikacji i anulowania uprawnień.

§ 4

STOSOWANE METODY I ŚRODKI UWIERZYTELNIANIA ORAZ PROCEDURY ZWIĄZANE Z ZARZĄDZANIEM I UŻYTKOWANIEM STOSOWANYCH METOD I ŚRODKÓW UWIERZYTELNIENIA

1. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
2. Zmiana hasła użytkownika następuje nie rzadziej niż co 30 dni.
3. Identyfikatora użytkownika nie należy zmieniać bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu nie powinien być on przydzielany innej osobie.
4. Użytkownicy są odpowiedzialni za zachowanie poufności swoich haseł.
5. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności, nie wolno ich udostępniać, ani zapisywać w sposób jawny.
6. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
7. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, użytkownik zobowiązany jest do jego natychmiastowej zmiany.
8. Przy wyborze hasła obowiązują następujące zasady:
    a) długość hasła: minimum 8 znaków,
    b) hasło powinno zawierać co najmniej jedną dużą literę, jedną cyfrę, jeden znak specjalny.
9. Zmiany hasła nie należy zlecać innym osobom.
10. W systemach umożliwiających zapamiętanie nazwy użytkownika lub jego hasła nie należy korzystać z tego ułatwienia.

§ 5

PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA, ZAKOŃCZENIA PRACY PRZEZNACZONE DLA UŻYTKOWNIKÓW SYSTEMU

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 poprzez zabezpieczony hasłem wygaszacz ekranu 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 wylogować się z sieci komputerowej.
5. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania oraz zakończeniem pracy w sieci.
6. Przypadki stwierdzenia nieprawidłowości w zakresie działania systemu należy zgłaszać do Administratora Systemu, który zdarzenia stanowiące incydenty bezpieczeństwa rejestruje w Dzienniku Systemu Informatycznego (tj. rejestrze incydentów).
7. Wzór dziennika zawiera **załącznik nr 15** do Polityki Bezpieczeństwa.
8. Zabronione jest podejmowanie działań mogących być zagrożeniem dla systemu, a w tym:
   - łamanie haseł,
   - dokonywanie włamań na konta innych użytkowników,
   - nieprawne uzyskiwanie dostępu do kont administracyjnych,
   - zakłócanie działania usług,
   - omijanie i badanie zabezpieczeń (nie dotyczy czynności wykonywanych w ramach audytu, czynności kontrolnych lub testowania wykonywanych przez osoby upoważnione),
   - doprowadzanie do rozprowadzania wirusów, robaków i koni trojańskich oraz niechcianej poczty,
   - praca na koncie innego użytkownika.

§ 6
PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA

1. Kopie są wykonywane zgodnie z harmonogramem. Mogą być również tworzone okazjonalnie przez użytkowników.
2. Za systematyczne tworzenie kopii zapasowych odpowiada Administrator Systemu Dziedzinowego.
3. W przypadku części aplikacji ich tworzenie odbywa się automatycznie po zakończeniu pracy. Mogą one być również wykonywane okazjonalnie przez użytkowników, w celu zabezpieczenia danych szczególnie istotnych dla działalności Uczelni.
4. Bazy danych, oprogramowanie oraz konfiguracja systemów powinny być zabezpieczone w postaci kopii bezpieczeństwa.
5. Należy wykonywać następujące kopie bezpieczeństwa:
   a) przed dokonaniem zmian w konfiguracji systemów lub oprogramowania,
   b) przed dokonaniem zmian w programach (np. zmiana wersji),
6. Za opracowanie i wdrożenie szczegółowych zasad i trybu wykonywania kopii zapasowych odpowiedzialny jest Administrator Systemu Dziedzinowego lub w ramach umowy wsparcia i utrzymania podmiot trzeci.

§ 7
SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI, ZAWIERAJĄCYCH DANE OSOBOWE, W TYM KOPII ZAPASOWYCH, ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA

I. Kopie zapasowe

1. Kopie zapasowe należy przechowywać w warunkach gwarantujących brak dostępu do nich osób nieupoważnionych, np. w zabezpieczonych pomieszczeniach, w sejfach lub szafach zamykanych na klucz.
2. W przypadku wykonywania zabezpieczeń długoterminowych lub na nośnikach zewnętrznych, np. taśmach, płytach CD, DVD nośniki te należy co kwartał sprawdzać pod kątem ich dalszej przydatności oraz odtwarzalności.
3. Kopie zapasowe zostają usunięte w przypadku ustania ich użyteczności.

II. Elektroniczne nośniki informacji. Komputery przenośne.

1. Dopuszcza się używanie służbowych urządzeń umożliwiających przenoszenie i archiwizowanie danych, w tym nagrywarek DVD, dysków zewnętrznych oraz nośników typu pendrive.
2. Zabrania się używania prywatnych nośników zewnętrznych.
3. Należy unikać przechowywania danych wrażliwych na nośnikach zewnętrznych takich jak np. pendrive-y.
4. W przypadku konieczności przechowywania na nośnikach, o których mowa w pkt 2 ważnych danych należy stosować wobec tych danych środki ochrony kryptograficznej.
5. Zabronione jest używanie pendrive-ów lub innych nośników do przenoszenia danych na prywatne komputery lub inne urządzenia mogące służyć do przechowywania danych.
6. Nośniki przenośne (takie jak pendrive-y) należy transportować w sposób bezpieczny (nie pozostawiać ich

w miejscach widocznych np. w samochodach, przypiętych do pasków itp.

7. W razie zaistnienia okoliczności uzasadniających konieczność wyniesienia nośnika poza obszar przetwarzania danych osobowych, jego użytkownik zobowiązany jest do zachowania szczególnej ostrożności i zabezpieczenia nośnika przed dostępem osób nieupoważnionych, utratą, modyfikacją lub zniszczeniem.
8. 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 w sposób uniemożliwiający ich odczytanie.
9. Urządzenia, dyski lub inne informatyczne nośniki, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymywania danych osobowych, pozbawia się wcześniej zapisu tych danych.
10. Urządzenia, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych, albo naprawia się je pod nadzorem osoby upoważnionej.
11. W przypadku konieczności przekazania nośników do podmiotu świadczącego usługę odzyskiwania danych należy bezwzględnie podpisać stosowną umowę zawierającą odpowiednie klauzule poufności, bądź umowę powierzenia.
12. Za czynności ujęte w pkt 9-11 odpowiedzialny jest Administrator Systemu Informatycznego.
13. Za bezpieczeństwo komputerów przenośnych odpowiedzialni są ich użytkownicy.
14. Komputery przenośne po zakończonej pracy winny być przechowywane w warunkach zapewniających ich bezpieczeństwo
15. W przypadku korzystania z komputerów przenośnych poza siedzibą Uczelni, należy używać ich w sposób uniemożliwiający odczyt danych z ekranu przez osoby postronne.
16. Podczas transportu komputerów przenośnych, wynoszonych poza obszar przetwarzania danych osobowych, należy zapewnić ich bezpieczeństwo, tj. nie należy ich pozostawiać bez nadzoru, np. w samochodzie (lub innym miejscu).
17. Należy unikać przechowywania na komputerach przenośnych danych osobowych lub innych ważnych danych.
18. W przypadku konieczności zapisania na komputerze przenośnym danych, należy stosować wobec tych danych środki ochrony kryptograficznej.
19. Komputery przenośne muszą być wyposażone w uaktywniony firewall programowy.
20. W razie przechowywania danych osobowych na dyskach lokalnych komputerów stacjonarnych, należy stosować zabezpieczenia wymagane dla systemów przetwarzających dane osobowe.

III. Wydruki

1. Poza elektroniczną formą danych osobowych przetwarzane są dane ze zbioru, w postaci wydruków zawierających dane osobowe. Są one przechowywane w miejscu uniemożliwiającym bezpośredni dostęp do nich osobom niepowołanym, tj. w zabezpieczonych pomieszczeniach, w szafach zamykanych na klucz. Pomieszczenia, w którym przechowywane są wydruki robocze, muszą być należycie zabezpieczone po godzinach pracy.
2. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

§ 8
SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO

1. Oprogramowanie stosowane w Uczelni może pochodzić wyłącznie ze źródeł legalnych i sprawdzonych, obowiązkowo posiadać łatwo dostępną informację o identyfikatorze, wersji i numerze licencji.
2. Wdrożenie modyfikacji istniejącego, lub stworzenie albo zakup nowego oprogramowania przetwarzającego dane osobowe możliwe jest wyłącznie w przypadku spełnienia przez przedmiotowe oprogramowanie wymogów z zakresu bezpieczeństwa, wynikających z obowiązujących przepisów prawa dotyczących ochrony danych osobowych.
3. Zabronione jest uruchamianie lub instalowanie i uruchamianie oprogramowania niezwiązanego merytorycznie z wykonywaną pracą.
4. Korzystanie z zasobów Uczelni poprzez sieć publiczną, winno mieć miejsce po zastosowaniu koniecznych systemów zabezpieczeń i mechanizmów ochronnych, w szczególności firewalli oraz systemu uwierzytelniania użytkowników i szyfrowania danych, a także kompleksowego oprogramowania antywirusowego.
5. Sieć wewnętrzna Uczelni odseparowana jest od sieci publicznej za pomocą firewalli sprzętowych i programowych.
6. Dostęp do sieci rozległej mogą posiadać, przy zastosowaniu zasad dopuszczenia do zasobów informatycznych obowiązujących w Uczelni:
   a) pracownicy Uczelni,
   b) studenci Uczelni,
   c) osoby lub podmioty, z którymi Uczelnia współpracuje na podstawie zawartych umów oraz ich pracownicy – w zakresie przewidzianym umową.
7. Za techniczne umożliwienie użytkownikom korzystania z zasobów internetowych odpowiedzialny

jest Administrator Systemu Informatycznego.

8. W celu ochrony systemu informatycznego przed szkodliwym oprogramowaniem, oprogramowanie antywirusowe podlegające systematycznej aktualizacji musi być zainstalowane na każdym stanowisku komputerowym przetwarzającym dane osobowe. Za prawidłowość realizacji powyższego obowiązku odpowiadają kierownicy poszczególnych jednostek organizacyjnych.
9. Sprawdzanie dostępności baz wirusów oprogramowania antywirusowego odbywa się automatycznie nie rzadziej niż raz na dobę. Zaleca się okresowe monitorowanie, czy aktualizacja ta przebiega bez zakłóceń.
10. Użytkownicy przetwarzający dane osobowe zobowiązani są do niezwłocznego zgłaszania do kierownika jednostki organizacyjnej, każdej stwierdzonej nieprawidłowości, dotyczącej profilaktyki antywirusowej (np. braku zainstalowanego oprogramowania antywirusowego, nieaktualności sygnatur wirusów).
11. Kierownik jednostki podejmuje działania mające na celu eliminację nieprawidłowości.
12. Wszystkie pliki otrzymywane z zewnątrz, jak również wysyłane na zewnątrz, należy sprawdzać pod kątem występowania wirusów najnowszą dostępną wersją programu antywirusowego.
13. Każdy użytkownik zobowiązany jest do ochrony przed szkodliwym oprogramowaniem powierzonego mu stanowiska komputerowego.
14. Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje użytkownik, który nośnik zamierza użyć.
15. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.
16. Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje pracownik, który pocztę otrzymał.
17. W przypadku stwierdzenia pojawienia się wirusa, każdy użytkownik winien:
    - odłączyć stanowisko komputerowe od sieci,
    - zawiadomić bezpośredniego przełożonego i Administratora Sieci Informatycznej o zaistniałym zdarzeniu,
    - zanotować nazwę wirusa, uruchomić program antywirusowy celem wykonania skanu dysku twardego.
18. W razie uszkodzenia danych lub programów, Administrator Systemu Informatycznego zobowiązany jest do przywrócenia sprawności systemu korzystając z kopii zapasowych.

§ 9
PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH

1. Przeglądy, konserwacje lub naprawy systemów i nośników wykorzystywanych w Uczelni dokonywane są przez osobę upoważnioną do tego typu czynności, w szczególności Administratora Systemu Informatycznego.
2. Dopuszcza się realizację czynności określonych w ustępie 1 przez specjalistyczne firmy świadczące usługi z zakresu IT. W przypadku korzystania z usług specjalistycznej firmy konieczne jest zawarcie stosownej umowy cywilnoprawnej.
3. Umowy dotyczące świadczenia usług teleinformatycznych, w tym zakupu, modernizacji, sprzedaży lub serwisu urządzeń komputerowych, systemów informatycznych i oprogramowania powinny zawierać niezbędne klauzule określające wzajemne prawa i obowiązki stron umowy, a w szczególności wymagania dotyczące bezpieczeństwa, dostępu i ochrony danych oraz zakresu odpowiedzialności stron umowy.
4. W przypadku zdalnego dostępu do komputera (np. w celu wykonywania czynności serwisowych na komputerze) użytkownik komputera musi potwierdzić przejęcie pulpitu komputera oraz nadzorować wszelkie czynności wykonywane przez Administratora Systemu Informatycznego lub osobę przejmującą pulpit komputera, której zostały zlecone stosowne działania.

§ 10
ZASTOSOWANE ŚRODKI BEZPIECZEŃSTWA

Opis poziomu bezpieczeństwa oraz zastosowanych środków bezpieczeństwa zawiera **załącznik nr 17** do Polityki Bezpieczeństwa, przedstawiający wymogi dotyczące środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności danych i ochrony systemów informatycznych przetwarzających dane osobowe.