Załącznik nr 1
do Zarządzenia Rektora nr 16/2018
z dnia 25.05.2018 r.

Regulamin przetwarzania danych osobowych przez osoby upoważnione do przetwarzania danych osobowych w kartotekach i systemach informatycznych Akademii Sztuk Pięknych w Warszawie „Akademia"

1. Osoby zatrudnione przy przetwarzaniu danych osobowych są zobowiązane do zachowaniu poufności wszelkich danych osobowych uzyskanych w toku czynności, w tym osobom, którym nie jest to niezbędne do realizacji ich zadań powierzonych przez Akademię.
2. Osoby zatrudnione przy przetwarzaniu danych osobowych są uprawnione i zobowiązane do konsultacji wszelkich zagadnień mających związek z danymi osobowymi z Inspektorem Ochrony Danych.
3. Osoby zatrudnione przy przetwarzaniu danych osobowych mają obowiązek zgłaszania zamiaru powierzenia przetwarzania danych osobowych podmiotom zewnętrznym i konsultacji z Inspektorem Danych Osobowych treści umów powierzenia przetwarzania danych osobowych.
4. Osoby zatrudnione przy przetwarzaniu danych osobowych są zobowiązane powiadomić Inspektora Danych osobowych o ewentualnych naruszeniach bezpieczeństwa systemu ochrony danych osobowych. Za zdarzenia naruszające bezpieczeństwo danych osobowych uważa się w szczególności:
   - nieupoważniony dostęp do danych osobowych,
   - ujawnienie bądź utrata danych osobowych,
   - nieupoważniona modyfikacja danych osobowych, kopiowanie lub niszczenie dokumentów zawierających dane osobowe,
   - inne naruszenie postanowień Rozporządzenia RODO.
5. Osobom zatrudnionym przy przetwarzaniu danych osobowych do przetwarzania danych osobowych zabrania się:
   a) przetwarzania danych osobowych:
      - które nie są niezbędne do prawidłowego wykonywania obowiązków pracowniczych,
      - niezgodnie z celem ich przetwarzania;
   b) udostępniania lub umożliwiania dostępu do danych osobowych osobom nieupoważnionym,
   c) niedopełniania obowiązku poinformowania osoby, której dane dotyczą, o przysługujących jej prawach,
   d) uniemożliwiania osobie, której dane dotyczą, korzystania z przysługujących jej praw.
6. Osoba zatrudniona przy przetwarzaniu danych osobowych niszczy zbędne dokumenty papierowe zawierające dane osobowe wyłącznie w niszczarkach.
7. Osoba zatrudniona przy przetwarzaniu danych osobowych nie pozostawia bez nadzoru sprzętu i dokumentów mu powierzonych.
8. Osoba zatrudnionym przy przetwarzaniu danych osobowych zabezpiecza pomieszczenie, w którym są przetwarzane przez niego dane osobowe, przed wstępem osób nieupoważnionych.
9. Osoba zatrudnionym przy przetwarzaniu danych osobowych nie pozostawia w pomieszczeniu bez nadzoru osób nieupoważnionych do przetwarzania danych osobowych.
10. Osoba zatrudniona przy przetwarzaniu danych osobowych, której udostępniono komputer przenośny nie pozostawia go bez nadzoru, korzysta z szyfrowania dysku.
11. Sprzęt komputerowy i oprogramowanie udostępniane są wyłącznie w celach

służbowych. Osoby, którym udostępniono sprzęt komputerowy i oprogramowanie są odpowiedzialne za prawidłowe wykorzystywanie sprzętu i oprogramowania zgodnie z tym celem.

12. Osoby zatrudnione przy przetwarzaniu danych osobowych nie są uprawnione do instalacji oprogramowania bez wiedzy i zgody osoby odpowiedzialnej za system informatyczny.
13. Pracownicy odpowiadają w pełni za skutki uruchomienia zainstalowanego przez siebie oprogramowania bez wiedzy osoby odpowiedzialnej za system informatyczny.
14. Przypadki instalowania i uruchomienia oprogramowania bez wiedzy służb informatycznych, w szczególności gdy jego uruchomienie wywołuje działania niedozwolone, traktowane jest jako celowe i świadome działanie pracownika zmierzające do zwiększenia ryzyka awarii systemów informatycznych.
15. Osoby zatrudnione przy przetwarzaniu danych osobowych nie powinni otwierać załączników w poczcie e-mail co do których mają uzasadnione podejrzenie co do ich pochodzenia. W takim przypadku powinny skonsultować się z osobą odpowiedzialną za system informatyczny
16. Osoby zatrudnione przy przetwarzaniu danych osobowych powinny stosować następujące postępowanie w stosunku do haseł dostępowych do stacji roboczej i aplikacji:
    a) hasło dostępu do stacji roboczej lub oprogramowania powinno składać się z co najmniej z 8 znaków (dużych i małych liter oraz z cyfr lub znaków specjalnych).
    b) dokonywać zmiany hasła, w przypadku, gdy nie jest to wymuszone przez system, nie rzadziej niż co 30 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione.
    c) Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: imion, nazwisk, inicjałów, dat, numerów rejestracyjnych samochodów, numerów telefonów. Hasło nie może być identyczne z loginem.
    d) Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności i odpowiada za wszystkie działania wykonane z wykorzystaniem osobistego loginu i hasła.
    e) Zabronione jest przekazywanie haseł innym osobom oraz zapisywanie haseł w sposób jawny (np. na karteczkach samoprzylepnych, w komputerze);
    f) w przypadku nadania pierwszego hasła lub zresetowania hasła przez Administratora Systemu Informatycznego należy je niezwłocznie zmienić.
17. Osoby zatrudnione przy przetwarzaniu danych osobowych stosują następująca zasady rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym:
    a) Użytkownik rozpoczyna pracę z systemem informatycznym przetwarzającym dane osobowe z użyciem identyfikatora i hasła.
    b) Podczas logowania należy zwracać uwagę na komunikaty systemu (np. czy ktoś nie próbował włamać się do systemu).
    c) Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. pracownikom innych działów) wglądu do danych wyświetlanych na monitorach komputerowych – tzw. polityka czystego ekranu.
    d) Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu.
    e) Po zakończeniu pracy, użytkownik zobowiązany jest:
        - wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,
        - zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne.
18. Osoby zatrudnione przy przetwarzaniu danych osobowych są zobowiązane do następującego korzystania z zasobów internetu:
    a) Pracownicy są zobowiązani do korzystania z serwisów internetowych zgodnie z zakresem swoich obowiązków, w celu realizacji zadań służbowych oraz zadań związanych z podnoszeniem kwalifikacji zawodowych.
    b) Zabrania się:

- korzystania z serwisów zawierających treści niecenzuralne lub w jakikolwiek sposób naruszające prawo;
- korzystania z serwisów niezwiązanych z obowiązkami pracownika, np. oferujących gry internetowe lub losowe, hazard, prywatne aukcje, rozrywkę, fora dyskusyjne, usługi chat;
- kopiowania i wysyłania plików o przeznaczeniu niewynikającym z wykonywanych zadań służbowych, w tym filmów, plików muzycznych, wygaszaczy oraz gier;
- umożliwiania osobom postronnym (w tym rodzinie i znajomym) dostępu do sieci wewnętrznej oraz do sieci internet przy wykorzystaniu udostępnionej infrastruktury technicznej;
- podłączenia komputera nie służącego do wykonywania obowiązków pracowniczych do sieci wewnętrznej bez uprzedniej pisemnej zgody administratora sieci.

19. Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane są do zachowania następujących zasad przy korzystaniu z poczty elektronicznej:
    a) użytkownicy nie mogą używać poczty elektronicznej do celów innych niż służbowe;
    b) zabrania się przesyłania dalej otrzymywanych wiadomości niezwiązanych z realizowaną pracą, np. reklam, "łańcuszków szczęścia", wiadomości obraźliwych, humorystycznych, pornograficznych;
    c) wysyłane załączniki, o ile to możliwe, powinny być skompresowane; załączniki zawierające dane osobowe powinny być szyfrowane, a hasło powinno być przekazane w bezpieczny sposób inną drogą np. sms.
    d) każdy użytkownik powinien archiwizować na swoim komputerze otrzymywane i wysyłane wiadomości;
    e) należy zwracać szczególną uwagę na wiadomości z nie znanych źródeł (adresów), w szczególności zawierających jakiekolwiek załączniki; w takich przypadkach użytkownicy nie powinni uruchamiać załączników (plików z rozszerzeniem typu: .exe, .com, .bat, .pif.
20. W celu zapewnienia bezpieczeństwa sieci oraz jej użytkowników zabrania się dokonywania następujących działań:
    a) instalowania oprogramowania o nieznanym działaniu, należy je traktować za potencjalnie szkodliwe;
    b) skanowania sieci informatycznej;
    c) prowadzenia wszelkiego rodzaju ataków ingerujących w działanie lub zasoby komputerów innych użytkowników lub urządzeń w sieci wewnętrznej, a także osób trzecich i urządzeń w Internecie;
    d) naruszania w jakikolwiek sposób bezpieczeństwa serwerów i ich bezawaryjnej pracy;
    e) zabrania się wykorzystywania narzędzi umożliwiających omijanie zabezpieczeń oraz ograniczeń sieci i systemów teleinformatycznych.
21. Wobec pracowników naruszających ww. zasady stosowane będą: blokady kont pocztowych, kont WWW i ftp, ograniczenie dostępu do Internetu (z całkowitą blokadą włącznie) oraz konsekwencje przewidziane przez kodeks pracy, kodeks cywilny oraz kodeks karny.
22. Niepodjęcie działań określonych niniejszym Regulaminem w przypadku stwierdzenia naruszenia ochrony danych osobowych stanowi naruszenie obowiązków pracownika.
23. W celu wprowadzenia szczegółowych zasad wprowadzone mogą być odrębne procedury.

REKTOR

prof. Adam Myjak