Załącznik do Zarządzenia nr 16/2010
Rektora Akademii Sztuk Pięknych w Warszawie
z dnia 12 kwietnia 2010 r.

Instrukcja Zarządzania Systemem Informatycznym Akademii Sztuk Pięknych w Warszawie

1. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności,
    a. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się:
        i. z niniejszym dokumentem
        ii. procedurami określonymi przez Administratora Bezpieczeństwa Informacji
        iii. posiadać upoważnienie do przetwarzania danych osobowych
    b. Zapoznanie się z powyższymi informacjami pracownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi załącznik do niniejszej instrukcji.
    c. Administrator Systemu Informatycznego przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnego upoważnienia (wniosku) określającego zakres uprawnień pracownika, którego wzór stanowi załącznik do niniejszej instrukcji.
    d. 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.
    e. Hasło ustanowione podczas przyznawania uprawnień przez Administratora Systemu Informatycznego należy zmienić na indywidualne podczas pierwszego logowania się w systemie.
    f. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.
    g. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
    h. W systemie informatycznym stosuje się uwierzytelnianie dwustopniowe na poziomie dostępu do systemu operacyjnego i sieci lokalnej oraz dostępu do aplikacji.
    i. Odebranie uprawnień pracownikowi następuje na pisemny wniosek przełożonego pracownika z podaniem daty oraz przyczyny odebrania uprawnień.
    j. Przełożony danego pracownika zobowiązany jest pisemnie informować Administratora Bezpieczeństwa Informacji o każdej zmianie dotyczącej pracownika mającej wpływ na zakres posiadanych uprawnień w systemie informatycznym.
    k. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie zablokować w systemie informatycznym oraz unieważnić hasło, dotyczy to także Administratora Systemów Informatycznych i jego zastępcy
    l. Administrator Systemu Informatycznego zobowiązany jest do prowadzenia i ochrony rejestru użytkowników i ich uprawnień w systemie informatycznym. rejestr stanowi załącznik nr 2,
    m. W sytuacjach awaryjnych np. w razie nieobecności Administrator Systemu Informatycznego wszelkie obowiązki przejmuje jego zastępca upoważniony przez Administratora Bezpieczeństwa Informacji
    n. Powyższe zasady nadawania/odbierania uprawnień dostępu do wszystkich systemów/aplikacji eksploatowanych w Akademii Sztuk Pięknych w Warszawie obowiązują wszystkich pracowników.
    o. W przypadku gdy system/aplikacja nie posiada wbudowanych mechanizmów kontroli dostępu, wówczas należy niezwłocznie rozbudować taki system/aplikacje o te mechanizmy, a do czasu

wdrożenia takich mechanizmów należy zaimplementować ograniczenia dostępu na poziomie systemu operacyjnego, bądź ograniczenia proceduralne.

2. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem
    a. Bezpośredni dostęp do systemu informatycznego może mieć miejsce wyłącznie po podaniu identyfikatora osoby i właściwego hasła.
    b. Administrator Systemu Informatycznego lub jego zastępca wyznacza hasło tymczasowe, przekazuje je w formie ustnej lub w postaci zaszyfrowanego pliku tekstowego, które po pierwszym zalogowaniu musi zostać zmienione.
    c. Hasło użytkownika musi być zmieniane co 30 dni.
    d. Identyfikator użytkownika nie może być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może zostać przydzielany innej osobie.
    e. Pracownicy są odpowiedzialni za zachowanie poufności swoich identyfikatorów i haseł.
    f. Hasła mogą być przechowywane tylko w postaci zaszyfrowanego pliku tekstowego wyłącznie przez pracownika, który posługuję się danym hasłem.
    g. Hasła niewolno przekazywać osobom trzecim, ani zlecać im jego zmiany.
    h. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
    i. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła i poinformowania o zaistniałym fakcie Administratora Bezpieczeństwa Informacji.
    j. Przy wyborze hasła obowiązują następujące zasady:
        i. minimalna długość hasła - 8 znaków,
        ii. hasło musi zawierać przynajmniej 1 małą, 1 dużą literę oraz 1 cyfrę lub znak specjalny
        iii. zakazuje się stosować: haseł, które użytkownik stosował uprzednio, swojego identyfikatora w jakiejkolwiek formie, swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiejkolwiek formie, imion (w szczególności imion osób z najbliższej rodziny), ogólnie dostępnych informacji o użytkowniku(numer telefonu, numer rejestracyjny samochodu, numeru PESEL,itp.)
3. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu informatycznego
    a. Rozpoczęciem pracy w systemie komputerowym wymaga zalogowania się do systemu przy użyciu indywidualnego identyfikatora oraz hasła dostępu.
    b. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
    c. Przed opuszczeniu stanowiska pracy należy zablokować stację roboczą lub wylogować się z oprogramowania i systemu operacyjnego.
    d. Przed wyłączeniem komputera należy bezwzględnie zakończyć prace uruchomionych programów, wylogować się z systemu operacyjnego i wykonać zamkniecie systemu
    e. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania isystemu operacyjnego.
    f. W przypadku stwierdzenia, że system operacyjny lub inny system informatyczny został uruchomiony bez wiedzy użytkownika danej stacji roboczej, należy o tym fakcie poinformować Administratora Systemu Informatycznego.
4. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania
    a. Całościowe kopie bezpieczeństwa zawierające zbiory danych osobowych i pliki programów służących do ich przetwarzania wykonywane są codzienne.

b. Za systematyczne przygotowanie kopii bezpieczeństwa odpowiada Administrator Systemu Informatycznego.

c. Kopie bezpieczeństwa wykonywane są poprzez sieć lokalną, wyizolowaną logicznie z sieci ogólnodostępnej, na dyski twarde serwerów backupowych.

d. Zachowuje się minimum 5 kopii bezpieczeństwa z poprzednich dni.

e. Dodatkowe zabezpieczenie wszystkich programów i danych wykonywane jest w pierwszym dniu każdego miesiąca w postaci zapisu na płytach DVD-R.

f. Dyski DVD lub dyski twarde uszkodzone lub niemożliwe do odczytania są niszczone fizycznie w sposób uniemożliwiający ich odczytanie.

5. Sposób, miejsce i okres przechowywania nośników elektronicznych zawierających dane osobowe oraz kopie bezpieczeństwa

a. Dane osobowe w postaci elektronicznej - za wyjątkiem kopii bezpieczeństwa –zapisane na dyskietkach, płytach CD/DVD czy dyskach twardych nie mogą opuścić obszaru przetwarzania danych osobowych.

b. Elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych, określony w Polityce bezpieczeństwa przetwarzania danych osobowych, w zamkniętych szafach lub sejfach.

c. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, niszczone fizycznie w sposób uniemożliwiający ich odczytanie.

d. Elektroniczne nośniki informacji, zawierające dane osobowe, nie mogą zostać przekazane innemu podmiotowi nieuprawnionemu do dostępu do tych danych , nawet po uprzednim usunięciu danych z nośnika.

e. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawa zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej.

f. Kopie bezpieczeństwa przechowywane są w pokoju nr 36 Budynku Rektoratu ASP.

g. Dostęp do kopii bezpieczeństwa ma Administrator Systemu Informatycznego oraz upoważnieni przez niego pracownicy.

h. W przypadku konieczności przechowywania wydruków zawierających dane osobowe są one przechowywane w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym, tj. w zamykanych szafkach lub sejfach w obszarze przetwarzania danych osobowych.

i. Pomieszczenie, w którym przechowywane są wydruki robocze musi być należycie zabezpieczone po godzinach pracy.

j. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie w specjalnej niszczarce.

6. Sposób zabezpieczenia systemu informatycznego przed działalnością szkodliwego oprogramowania

a. Na każdym stanowisku komputerowym jest zainstalowane oprogramowanie antywirusowe Eset Nod32 z włączoną ochroną antywirusową i antyspyware oraz zapora ogniowa uniemożliwiająca nawiązanie połączenia z chronionymi komputerami oraz blokujące ruch o charakterze niepożądanym lub takim, który może zostać uznany za szkodliwy

b. Definicje wzorców wirusów aktualizowane są codziennie.

c. Każdy e-mail wpływający/wypływająca z/do konta pocztowego ASP jest sprawdzany pod kątem występowania oprogramowania szkodliwego przez oprogramowanie antywirusowe zlokalizowane lokalnie na stacji roboczej i serwerze pocztowym.

d. Bezwzględnie zabrania się otwierania i przekazywania wiadomości pocztowych email , niewiadomego pochodzenia.

e. Bezwzględnie zabrania się używania nośników elektronicznych niewiadomego pochodzenia.

f. Bezwzględnie zabrania się pobierania z sieci Internet, tam gdzie jest dostępna, plików niewiadomego pochodzenia.

g. W przypadku zauważenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub jego oprogramowania należy zgłosić ten fakt lokalnemu informatykowi.

h. W przypadku wykrycia szkodliwego oprogramowania należy zgłosić ten fakt lokalnemu informatykowi.

7. Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych

   a. Dane osobowe mogą być udostępniane wyłącznie osobom upoważnionym na podstawie upoważnienia wydanego przez Administratora Bezpieczeństwa Informacji.

   b. Udostępnienie danych osobą upoważnionym powinno być odnotowywane w rejestrze zawierającym nazwę jednostki organizacyjnej lub imieniu i nazwisku osoby, której udostępniono dane, zakresie udostępnianych danych, dacie udostępnienia.

   c. Obowiązek odnotowania ww. informacji w Rejestrze spoczywa na użytkowniku systemu udostępniającemu dane.

   d. Odnotowanie informacji w Rejestrze powinno nastąpić niezwłocznie po udostępnieniu danych.

   e. Udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

   f. Na żądanie osoby, której dane zostały udostępnione, informacje o udostępnionych danych są zamieszczane w raporcie z Rejestru, a raport przekazywany tej osobie.

   g. Nadzór nad prawidłowością odnotowywania w Rejestrze ww. informacji sprawuje Administrator Bezpieczeństwa Informacji.

8. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

   a. Przeglądy i konserwacja urządzeń oraz programów użytkowanych po przetwarzania danych osobowych wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonych przez producenta sprzętu lub oprogramowania.

   b. Nieprawidłowości ujawnione w trakcie tych działań powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. O fakcie ujawnienia nieprawidłowości należy zawiadomić Administratora Bezpieczeństwa Informacji.

   c. Jeśli producent nie przewidział dla danego urządzenia/programu potrzeby dokonywania przeglądów eksploatacyjnych, lub też nie określił ich częstotliwości, to o dokonaniu przeglądu oraz sposobie jego przeprowadzenia decydują Administratora Bezpieczeństwa Informacji.

   d. Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada przełożony Administratora Bezpieczeństwa Informacji.

   e. Przeglądy i konserwacja urządzeń oraz programów użytkowanych po przetwarzania danych osobowych wchodzących w skład systemu informatycznego dokonywane przez firmy zewnętrzne mogą być dokonywane pod nadzorem Administratora Systemu Informatycznego lub po usunięciu z nośników danych osobowych