INSTRUKCJA DOTYCZĄCA ODPOWIEDZIALNOŚCI UŻYTKOWNIKÓW ZA BEZPIECZEŃSTWO KOMPUTERÓW W ZAKRESIE ADMINISTRACJI DANYMI OSOBOWYMI

Bezpieczne hasło

- Każdy użytkownik systemu informatycznego posiada własne hasło i identyfikator.
- Hasło ustanowione podczas przyznawania uprawnień należy zmienić na indywidualne podczas pierwszego logowania się w systemie informatycznym.
- Użytkownik ponosi odpowiedzialność za wszelkie operacje wykonywane przy użyciu jego identyfikatora i hasła.
- Zmiana hasła użytkownika następuje nie rzadziej niż co 30 dni.
- Przy wyborze hasła obowiązują następujące zasady:
  - minimalna długość hasła – 8 znaków,
  - właściwa złożoność hasła - litery duże i małe oraz cyfry i znaki specjalne, o ile system informatyczny na to pozwala.
- Zakazuje się stosować haseł:
  - które użytkownik stosował uprzednio (do dziesięciu haseł wstecz),
  - będących nazwą użytkownika w jakiejkolwiek formie (np. pisanej dużymi literami),
  - analogicznych jak identyfikator,
  - zawierających ogólnie dostępne informacje, takie jak: imię, nazwisko, numer rejestracyjny samochodu, numer telefonu, imiona dzieci itp.,
  - stanowiących wyrazy słownikowe lub przewidywalne sekwencje znaków, np. 12345678 lub abcdefgh.
- Zmiany hasła nie należy zlecać innym osobom.
- W systemach umożliwiających zapamiętanie nazwy użytkownika lub jego hasła nie należy korzystać z tego ułatwienia.
- Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
- W sytuacji kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, użytkownik zobowiązany jest do jego natychmiastowej zmiany.
- Użytkownicy są odpowiedzialni za zachowanie poufności swoich haseł.
- Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności, nie wolno ich udostępniać, ani zapisywać w sposób jawny.

Bezpieczne logowanie

- Przed rozpoczęciem pracy w systemie komputerowym należy zalogować się do systemu przy użyciu indywidualnego identyfikatora oraz hasła.
- 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.
- Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązana jest wykonać funkcję wylogowania z systemu.
- Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów, wykonać zamknięcie systemu i wylogować się z sieci komputerowej.

Bezpieczna praca z systemem

- 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, włącznie ze zwolnieniem w trybie dyscyplinarnym.
- 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.

Bezpieczna praca z oprogramowaniem i siecią publiczną

- Zabronione jest uruchamianie lub instalowanie i uruchamianie oprogramowania niezwiązanego merytorycznie z wykonywaną pracą.
- Każdy użytkownik zobowiązany jest do ochrony przed szkodliwym oprogramowaniem powierzonego mu stanowiska komputerowego.
- Użytkownicy zobowiązani są do niezwłocznego zgłaszania do kierownika jednostki organizacyjnej każdej stwierdzonej nieprawidłowości dotyczącej profilaktyki antywirusowej (np. braku

zainstalowanego oprogramowania antywirusowego, nieaktualności sygnatur wirusów).

- Korzystanie z zasobów Uniwersytetu poprzez sieć publiczną winno mieć miejsce po zastosowaniu koniecznych systemów zabezpieczeń i mechanizmów ochronnych, w szczególności firewall-i oraz systemu uwierzytelniania użytkowników i szyfrowania danych, a także kompleksowego oprogramowania antywirusowego.
- W przypadku konieczności dokonania rejestracji w Internecie zabronione jest wykorzystywanie do tego celu identyfikatorów i haseł używanych do dostępu do zasobów Uniwersytetu.
- Wszystkie pliki otrzymywane z zewnętrz, jak również wysyłane na zewnątrz, należy sprawdzać pod kątem występowania wirusów najnowszą dostępną wersją programu antywirusowego.
- Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.
- Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje pracownik, który pocztę otrzymał.
- W przypadku stwierdzenia pojawienia się wirusa, każdy użytkownik winien:
    - odłączyć stanowisko komputerowe od sieci,
    - zawiadomić przełożonego i jednostkę LubMAN UMCS o zaistniałym zdarzeniu,
    - zanotować nazwę wirusa, uruchomić program antywirusowy celem wykonania skanu dysku twardego.

Bezpieczne dane na komputerach przenośnych

- Za bezpieczeństwo komputerów przenośnych odpowiedzialni są ich użytkownicy.
- Komputery przenośne po zakończonej pracy winny być przechowywane w warunkach zapewniających ich bezpieczeństwo (szafy zamykane na klucz).
- W przypadku korzystania z komputerów przenośnych poza siedzibą Uniwersytetu należy używać ich w sposób uniemożliwiający odczyt danych z ekranu przez osoby postronne.
- Podczas transportu komputerów przenośnych wynoszonych poza obszar przetwarzania danych osobowych należy zapewnić ich bezpieczeństwo, tj. nie należy ich pozostawiać bez nadzoru w samochodzie (lub innym miejscu). Muszą one być przewożone jako bagaż podręczny.
- Należy unikać przechowywania na komputerach przenośnych danych osobowych lub innych ważnych danych.
- W przypadku konieczności zapisania na komputerze przenośnym danych osobowych lub innych ważnych danych należy stosować wobec tych danych środki ochrony kryptograficznej.
- Komputery przenośne muszą być wyposażone w uaktywniony firewall programowy.

Bezpieczne dane na nośnikach przenośnych

- Należy unikać przechowywania ważnych danych na nośnikach zewnętrznych, takich jak np. pendrive-y.
- W przypadku konieczności przechowywania na nośnikach, o których mowa w pkt. powyżej ważnych danych należy stosować wobec tych danych środki ochrony kryptograficznej.
- Zabronione jest używanie pendrive-ów lub innych nośników do przenoszenia danych na prywatne komputery lub inne urządzenia mogące służyć do przechowywania danych.
- Nośniki przenośne (takie jak pendrive-y) należy transportować w sposób bezpieczny (nie pozostawić ich w miejscach widocznych, np. w samochodach, przypiętych do pasków itp.

PRZYPOMINAMY:

1. 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, włącznie ze zwolnieniem w trybie dyscyplinarnym.
2. Użytkownik ponosi odpowiedzialność za wszelkie operacje wykonywane przy użyciu jego identyfikatora i hasła.
3. Użytkownicy są odpowiedzialni za zachowanie poufności swoich haseł.
4. Za bezpieczeństwo komputerów przenośnych odpowiedzialni są ich użytkownicy.