

## ***Instrukcja postępowania w przypadkach naruszenia ochrony danych osobowych w Uniwersytecie Przyrodniczym we Wrocławiu***

### § 1

Za naruszenie ochrony danych osobowych uznaje się przypadki, gdy:

- a) stwierdzono naruszenie zabezpieczenia systemu informatycznego,
- b) 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.

### § 2

Pracownik lub doktorant Uczelni, który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych w systemie informatycznym Uczelni zobowiązany jest, a student uprawniony, do niezwłocznego poinformowania o tym administratora tego systemu, lokalnego administratora danych osobowych, a w przypadku jego nieobecności – ABI Uczelni.

### § 3

Administrator danych osobowych, który stwierdził lub uzyskał informację wskazującą na naruszenie zasad ochrony tych danych zobowiązany jest do niezwłocznego:

- 1) zapisania wszelkich informacji i okoliczności związanych z danym zdarzeniem, a w szczególności dokładnego czasu uzyskania informacji o naruszeniu zasad ochrony danych osobowych lub czasu samodzielnego wykrycia tego faktu,
- 2) jeżeli zasoby systemu na to pozwalają, wygenerowania i wydrukowania wszystkich dokumentów i raportów, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzenia ich datą i podpisania,
- 3) przystąpienia do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym do określenia skali zniszczeń, metody dostępu osoby niepowołanej do danych itd.,
- 4) podjęcia odpowiednich kroków w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych, w tym między innymi:
  - a) fizycznego odłączenia urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie niepowołanej,
  - b) wylogowania użytkownika podejrzanego o naruszenie zasad ochrony danych,
  - c) zmianę hasła użytkownika (na konto administratora), poprzez którego uzyskano nielegalny dostęp, w celu uniknięcia ponownej próby uzyskania takiego dostępu.
- 5) szczegółowej analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia zasad ochrony danych osobowych,
- 6) przywrócenia normalnego działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, odtworzenia jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności mających na celu uniknięcie ponownego uzyskania dostępu przez osobę nieupoważnioną, tą samą drogą.

### § 4

Po przywróceniu normalnego stanu systemu informatycznego należy przeprowadzić szczegółową analizę, w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia, oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

Jeżeli przyczyną zdarzenia był błąd użytkownika systemu informatycznego, należy przeprowadzić szkolenie wszystkich osób biorących udział w przetwarzaniu danych.

Jeżeli przyczyną zdarzenia była infekcja wirusem należy ustalić źródło jego pochodzenia i wykonać zabezpieczenia antywirusowe i organizacyjne wykluczające powtórzenie się podobnego zdarzenia w przyszłości.

Jeżeli przyczyną zdarzenia okazało się zaniedbanie ze strony użytkownika systemu, należy wyciągnąć konsekwencje dyscyplinarne wynikające z kodeksu pracy oraz ustawy.

#### § 5

Lokalny administrator systemu informatycznego, w którym nastąpiło naruszenie zasad ochrony danych osobowych, w porozumieniu z właściwym lokalnym administratorem danych osobowych zobowiązany jest do przygotowania szczegółowego raportu o przyczynach, przebiegu i wnioskach ze zdarzenia i w terminie 14 dni od daty jego zaistnienia, przekazania go ABI.

#### § 6

ABI zobowiązany jest do przeprowadzania analiz raportów pochodzących od lokalnych administratorów systemów informatycznych i uwzględniania ich przy opracowywaniu corocznego raportu dla ADO Uczelni.