Załącznik nr 3
Do Zarządzenia nr ....25..../.2003.
Starosty Poznańskiego
Z dnia ...22.09.2003r.

Instrukcja postępowania w sytuacji naruszenia systemu ochrony danych osobowych

Starostwo Powiatowe w Poznaniu

STAROSTA POZNAŃSKI
.....
Jan Grabkowski Starosta

Opracował:

Marek Jóźwiak
Piotr Siwczak

§ 1

Podstawę prawną do niniejszej instrukcji stanowią:

1) ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883),

2) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przechowywania danych osobowych (Dz. U. Nr 80, poz. 521),

3) regulamin ochrony danych osobowych w Starostwie Powiatowym w Poznaniu.

§ 2

Niniejsza instrukcja określa zasady postępowania w sytuacji naruszenia systemu ochrony danych osobowych, w szczególności , 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 telekomunikacyjnej, mogą wskazywać na naruszenie zabezpieczeń tych danych.

§ 3

Za bezpieczeństwo danych osobowych przetwarzanych w Starostwie Powiatowym w Poznaniu odpowiada administrator bezpieczeństwa informacji.

§ 4

Każda osoba zatrudniona w Starostwie, która stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych w systemie informatycznym, powinna niezwłocznie poinformować o tym administratora bezpieczeństwa informacji (tel. 521), albo pełnomocnika ochrony (tel. 503)albo inną upoważnioną przez niego osobę.

§ 5

Osoba zatrudniona przy przetwarzaniu danych osobowych, która uzyskała informację lub sama stwierdziła naruszenie zabezpieczenia bazy danych osobowych w systemie informatycznym, zobowiązana jest niezwłocznie powiadomić o tym administratora bezpieczeństwa informacji w Starostwie lub pełnomocnika ochrony lub inną upoważnioną przez niego osobę, a w przypadku ich nieobecności - bezpośrednio administratora danych osobowych (Starostę).

§ 6

Administrator bezpieczeństwa informacji lub inna upoważniona , przez niego osoba powinna w pierwszej kolejności:

1) zapisać wszelkie informacje związane z danym zdarzeniem, a szczególnie: dokładny czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych i czas samodzielnego wykrycia tego faktu,

2) na bieżąco wygenerować i wydrukować (jeżeli zasoby systemu na to pozwalają) wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrzyć je datą i podpisem,

3) przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby niepowołanej.

§ 7

Niezwłocznie należy podjąć odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu do danych osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów jej ingerencji, szczególnie przez:
a) fizyczne odłączenie urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nieupoważnionej,
b) zmianę hasła na konto administratora i użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania.

§ 8

Po wyeliminowaniu bezpośredniego zagrożenia należy przeprowadzić wstępną analizę stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych w systemie

§ 9

Administrator bezpieczeństwa informacji lub inna upoważniona przez niego osoba powinna sprawdzić:
a) stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
b) zawartość zbioru danych osobowych,
c) sposób działania programu,
d) jakość komunikacji w sieci telekomunikacyjnej,
e) jak również wykluczyć możliwość obecności wirusów komputerowych.

§ 10

Po dokonaniu powyższych czynności administrator bezpieczeństwa informacji powinien przeprowadzić szczegółową analizę stanu systemu informatycznego obejmującego identyfikację:
- metody zaistniałego zdarzenia,
- metody dostępu do danych osoby nieupoważnionej,
- skali zniszczeń.

§ 11

Niezwłocznie należy przywrócić normalny stan działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, niezbędne jest odtworzenie jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności. mających na celu uniknięcie ponownego uzyskania dostępu tą samą drogą przez osobę niepowołaną.

§ 12

Po przywróceniu prawidłowego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę, w celu określenia przyczyny naruszenia ochrony danych osobowych oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości:
1) jeżeli przyczyną zdarzenia był błąd osoby zatrudnionej przy przetwarzaniu danych osobowych w systemie informatycznym, należy przeprowadzić dodatkowe szkolenie wszystkich osób biorących udział przy przetwarzaniu danych,
2) jeżeli przyczyną zdarzenia było uaktywnienie wirusa, należy ustalić źródło jego pochodzenia oraz wykonać zabezpieczenia antywirusowe,
3) jeżeli przyczyną zdarzenia było zaniedbanie ze strony osoby zatrudnionej przy przetwarzaniu danych osobowych, należy wyciągnąć konsekwencje regulowane

ustawą,

4) jeżeli przyczyną zdarzenia było włamanie w celu pozyskania bazy danych osobowych, należy dokonać szczegółowej analizy wdrożonych środków zabezpieczających, w celu zapewnienia skuteczniejszej ochrony bazy danych,
5) jeżeli przyczyną zdarzenia był zły stan urządzenia lub sposób działania programu, należy wówczas niezwłocznie przeprowadzić kontrolne czynności serwisowo-programowe.

§ 13

Administrator bezpieczeństwa informacji przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia (dołączając ewentualne kopie dowodów dokumentujących to zdarzenie) konsultuje go z pełnomocnikiem ochrony oraz w określonym terminie od daty zaistnienia, przekazuje go administratorowi danych osobowych - Staroście.

§ 14

Niniejsza instrukcja wchodzi w życie z dniem ....22.09.2003r.....

STAROSTA POZNAŃSKI
Jan Grabkowski