Załącznik nr 3
do Zarządzenie nr 7/08
Burmistrza Kamieńska
z dnia 28 stycznia 2008r.

Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych

I. Postanowienia ogólne.

1. Instrukcja określa tryb postępowania w sytuacji naruszenia ochrony danych osobowych gromadzonych i przetwarzania zarówno w zbiorach informatycznych, jak i w zbiorach manualnych. Instrukcję stosuje się także w przypadku, gdy stwierdzono naruszenie zabezpieczeń sprzętu informatycznego, sieci komputerowej, systemu alarmowego i zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe.

2. Przez naruszenie ochrony danych osobowych rozumie się niezgodne z przepisami ustawy o ochronie danych i rozporządzeń wykonawczych, przetwarzanie danych (zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie) oraz usuwanie (zmiana lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą).

3. Osobami bezpośrednio odpowiedzialnymi za zgodną z prawem ochronę danych osobowych i ich zabezpieczenie są:

- pracownicy upoważnieni do przetwarzania danych osobowych,
- kierownicy komórek organizacyjnych,
- administrator bezpieczeństwa informacji - w przypadku naruszenia systemów informatycznych.

II. Tryb postępowania w sytuacji naruszenia ochrony danych osobowych.

Każdy pracownik Urzędu Miejskiego, który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych w systemie informatycznym , powinien:

a) powstrzymać się od rozpoczęcia lub kontynuowania jakiejkolwiek czynności lub pracy mogącej spowodować zatarcie śladów bądź dowodów naruszenia,
b) podjąć, stosownie do zaistniałej sytuacji, niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować naruszeniem danych osobowych,
c) niezwłocznie powiadomić o zdarzeniu przełożonego, a gdy dotyczy to danych utrwalonych w zbiorach informatycznych administratora bezpieczeństwa informacji

Administrator bezpieczeństwa informacji, który stwierdził lub uzyskał informację wskazującą na naruszenie ochrony tej bazy danych zobowiązany jest do niezwłocznego:

1. zarejestrować zgłoszenie w odpowiednim rejestrze odnotowując wszelkie informacje i okoliczności związane z danym zdarzeniem, a w szczególności dokładny czas uzyskania informacji o naruszeniu ochrony danych osobowych lub samodzielnym wykryciu tego faktu, dane osoby zgłaszającej, datę i godzinę zgłoszenia oraz jego treść,
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 itp.
4. podjęcia odpowiednich kroków w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia
5. ochrony danych, w tym m.in.
    a) fizycznego odłączenia urządzeń i segmentów sieci które mogły umożliwić dostęp do bazy danych osobie niepowołanej,
    b) wylogowania użytkownika podejrzanego o naruszenie ochrony danych,
    c) zmianę hasła na konto administratora i użytkownika poprzez którego uzyskano nielegalny dostęp w celu uniknięcia ponownej próby uzyskania takiego dostępu.
6. szczegółowej analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych,
7. 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.

Po przywróceniu normalnego stanu bazy danych osobowych 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 było zaniedbanie ze strony użytkownika systemu należy wyciągnąć konsekwencje dyscyplinarne wynikające z kodeksu pracy oraz ustawy o ochronie danych osobowych.

Administrator Bezpieczeństwa Informacji sporządza z przebiegu zdarzenia raport, w którym zamieszcza, w szczególności informacje o :

1. ustaleniach dotyczących sytuacji naruszenia ochrony danych osobowych,
2. przeprowadzonych czynnościach,
3. podjętych decyzjach i ich uzasadnieniu,
4. wnioski i propozycje ewentualnego podniesienia zabezpieczeń w systemie przetwarzania

BURMISTRZ
mgr inż. Grzegorz Turlejski

INFORMATYK
mgr Mariusz Sewerynek

RADCA PRAWNY
mgr Urszula Kowalska-Smuga