Załącznik nr 2
do Zarządzenie nr 7/08
Burmistrza Kamieńska
z dnia 28 stycznia 2008r.

INSTRUKCJA
określająca sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem bezpieczeństwa informacji.

I. Stosowane metody i środki uwierzytelniania:

1. W systemie informatycznym stosowane jest uwierzytelnianie użytkownika przy pomocy jego identyfikatora i hasła.
2. Każdy użytkownik systemu posiada swój unikalny identyfikator.
3. Użytkownicy nie mogą używać tych samych identyfikatorów, ani wymieniać się identyfikatorami.
4. Hasło nie może być takie samo jak identyfikator.
5. Za gospodarkę hasłami odpowiedzialny jest Administrator Bezpieczeństwa Informacji
6. Hasło nie może być zapisywane w miejscu dostępnym dla osób nieuprawnionych.
7. Hasło użytkownika powinno mieć minimum 5 znaków.
8. Użytkownik nie może udostępnić identyfikatora, hasła i stanowiska roboczego osobom nieuprawnionym.
9. Hasło przy wpisywaniu nie może być wyświetlane na ekranie
10. Hasło użytkownika, umożliwiające dostęp do systemu informatycznego, utrzymuje się w tajemnicy, również po upływie jego ważności.
11. Pojedyncze komputery, na których dane osobowe służą do edycji powinny być zabezpieczone hasłem. Pracownicy zatrudnieni przy ich obsłudze nie mogą zezwalać na użytkowanie komputera osobom nieupoważnionym.
12. W przypadku czasowego opuszczenia stanowiska pracy, użytkownik systemu powinien wylogować się z systemu lub uruchomić wygaszacz ekranu zabezpieczony hasłem
13. Komputery nie pracujące w sieci muszą mieć hasło założone na BIOS
14. Zabrania się wprowadzania i zmiany haseł bez zgody Administratora Bezpieczeństwa Informacji

II. Korzystającym z systemu informatycznego w Urzędzie zabrania się:

1. udostępniania stanowiska pracy oraz istniejących w nich danych osobom nieupoważnionym;
2. udostępniania osobom nieuprawnionym programów komputerowych;
3. używania oprogramowania w innym zakresie niż pozwala na to umowa licencyjna;
4. przenoszenia programów komputerowych, dysków twardych z jednego stanowiska na inne;
5. samowolnego instalowania i używania programów komputerowych; programy komputerowe instalowane są przez administratora systemu lub za jego zgodą przez inną upoważnioną osobę;

6. używania nośników danych udostępnionych przez osoby nieuprawnione;
7. używania nośników danych niesprawdzonych, niewiadomego pochodzenia lub niezwiązanych z pracą; w przypadku konieczności użycia niesprawdzonych przenośnych nośników danych, należy te nośniki przeskanować programem antywirusowym; jeżeli program antywirusowy nie jest zainstalowany na danej stacji roboczej należy to zrobić na innym stanowisku;
8. wykorzystywania sieci komputerowej w celach innych, niż wyznaczone przez administratora.
9. nie wolno instalować w sieci własnego oprogramowania bez zgody Administratora Bezpieczeństwa Informacji
10. obowiązuje zasada „wszystko co nie jest dozwolone, jest zabronione”,

III. Procedury rozpoczęcia i zakończenia pracy.

1. Dane osobowe są przetwarzane z użyciem systemu informatycznego w godzinach pracy Urzędu Miasta; poza tymi godzinami wyłącznie w uzasadnionych przypadkach, po uzyskaniu pisemnej zgody Administratora Bezpieczeństwa Informacji, z zachowaniem warunków określonych w Regulaminie pracy Urzędu w formie upoważnienia jednorazowego lub stałego
2. Użytkownik ma obowiązek wylogowania się z systemu przy rozpoczęciu dłuższej nieobecności na stanowisku pracy lub zakończeniu tej pracy. Stanowisko komputerowe z uruchomionym systemem nie może pozostać bez kontroli pracującego na nim pracownika.
3. Wydruki zawierające dane osobowe należy przechowywać w miejscu uniemożliwiającym ich odczytanie przez osoby nieuprawnione. Wydruki nieprzydatne należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.
4. Przebywanie osób nieuprawnionych do dostępu do danych osobowych w pomieszczeniach znajdujących się na obszarze, w którym są przetwarzane dane osobowe, jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych.
5. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych w sposób uniemożliwiający dostęp do nich osób trzecich.
6. Korzystanie z zewnętrznych nośników informacji (dyskietek, dysków wymiennych itp.) może mieć miejsce wyłącznie po uzyskaniu zgody Administratora Bezpieczeństwa Informacji

IV. Metoda i częstotliwość tworzenia kopii awaryjnych.

1. za sporządzanie i bezpieczeństwo kopii odpowiedzialny jest Administrator Bezpieczeństwa Informacji lub inna osoba przez niego upoważniona,
2. kopii należy dokonywać poprzez przegrywanie całej bazy danych (bez kompresji),
3. kopie awaryjne może tworzyć jedynie Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona,
4. w czasie tworzenia kopii awaryjnej przez Administratora, dostęp do bazy dla wszystkich użytkowników powinien być zablokowany,

5. nośniki informacji z kopiami bezpieczeństwa powinny być wyjęte z komputera w czasie bieżącej pracy.
6. kopie zapasowe przechowywane są w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem, kopie te usuwa się niezwłocznie po ustaniu ich użyteczności,
7. Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu. Nośniki danych po ustaniu ich użyteczności należy pozbawiać danych lub niszczyć w sposób uniemożliwiający ich odczyt.

V. Sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych.

1. przeglądu i konserwacji dokonuje Administrator lub osoba przez niego upoważniona
2. w przypadku przekazywania komputera z dyskiem lub innym nośnikiem danych osobowych do naprawy, należy nośnik zdemontować, zabezpieczyć dostęp hasłem lub dokonać naprawy w obecności osoby upoważnionej przez Administratora danych, w przypadku przekazania nośnika innemu podmiotowi należy dane nieodwracalnie skasować
3. wszelkich nieprawidłowościach, awariach, próbie lub naruszeniu bezpieczeństwa danych osobowych, użytkownik powinien niezwłocznie powiadomić Administratora Bezpieczeństwa Informacji
4. zabronione jest dokonywanie napraw sprzętu komputerowego samodzielnie przez pracowników urzędu, bez zgody Administratora Bezpieczeństwa Informacji,

BURMISTRZ
mgr inż. Grzegorz Turlejski

INFORMATYK
Dariusz Sewerynek

RADCA PRAWNY
mgr Urszula Kowalska-Smęga