Załącznik nr 5 do
Zarządzenia nr ...../2010
Dyrektora Miejskiego Ośrodka
Pomocy społecznej w Lubaniu

Opis systemu służącego ochronie danych i ich zbiorów, w tym dowodów księgowych, ksiąg rachunkowych i innych dokumentów stanowiących podstawę dokonanych w nich zapisów

1. Osobą odpowiedzialną za system komputerowy i jego ochronę ustala się administratora systemu informatycznego, którym jest informatyk
2. Bezpieczna informacja komputerowa to taka, która jest chroniona przed nieupoważnionym odczytem i modyfikacją (tj. polegająca na poufności i integralności) oraz, która jest dostępna i wiarygodna dla uprawnionego użytkownika (tj. polegająca na dostępności i spójności).
3. Poufność informacji komputerowej polega na ochronie informacji komputerowej, ochronie danych itp. przed nieuprawnionym dostępem. Natomiast integralność to odporność informacji na nieuprawnioną modyfikację. Z kolei dostępność, polega na nieograniczonej możliwości korzystania przez uprawnionych użytkowników. Spójność oznacza konieczność spełnienia przez system komputerowy warunków określających zależności strukturalne jej składowych.
4. Należy chronić wszelkie zasoby takie jak: oprogramowanie, dane, sprzęt, zasoby administracyjne, fizyczne, występujące w systemie informatycznym lub działalności informatycznej.
5. System informatyczny spełnia kryteria: poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności. Kryterium poufności polega na ochronie przed ujawnieniem informacji nieuprawnionemu odbiorcy. Kryterium integralności tj. ochrona przed modyfikacją lub zniekształceniem aktywów przez osobę nieuprawnioną. Kryterium dostępności polega na zagwarantowaniu uprawnionego dostępu do informacji przy zachowaniu określonych rygorów czasowych. Kryterium rozliczalności to określenie i weryfikowanie odpowiedzialności za działania, usługi i funkcje realizowane za pośrednictwem systemu. Kryterium autentyczności to możliwość weryfikacji tożsamości podmiotów lub prawdziwości aktywów systemu. Kryterium niezawodności to gwarancja odpowiedniego zachowania się systemu i otrzymanych wyników.
6. Do najważniejszych zagrożeń, należą:
   - przechwycenie informacji – naruszenie poufności,
   - modyfikacja informacji – naruszenie integralności,
   - zniszczenie informacji – naruszenie dostępności,
   - blokowanie dostępu do informacji – naruszenie dostępności
7. Klasyfikacja powyższych zagrożeń:
   1. Ze względu na źródło zagrożenia na:
      a) wewnętrzne
      b) zewnętrzne
   2. Ze względu na celowość działań na:
      a) przypadkowe
      b) celowe
   3. Ze względu na rodzaj zagrożenia na:
      a) programowe
      b) sprzętowe
8. Pierwszym podstawowym zabezpieczeniem danych jest używanie hasła przy rozpoczęciu pracy
   z komputerem. Hasło to nie powinno być zbyt proste: zawiera osiem znaków, jednocześnie małe i wielkie litery czy liczby, nie można go znaleźć w słowniku. Hasło to powinno być zmieniane raz w miesiącu. Nawet przy krótkim odejściu użytkownika komputera, na przykład po to by zrobić sobie kawę, jego komputer powinien blokować się i wymagać znów wpisania hasła; można to zrobić przy pomocy zwykłego wygaszacza ekranu. Hasło to chroni dane znajdujące się na naszym komputerze.
9. Hasła mogą być również stosowane na niższych poziomach - opatrzone hasłem mogą być pojedyncze pliki zawierające dane, takie jak arkusze kalkulacyjne z planami finansowymi czy bazy z danymi osobowymi.

10. By hasło mogło być skuteczne, musi być tajne - nie można ich nikomu podawać, czy zapisywać
w łatwych do znalezienia miejscach.
11. W sieciach komputerowych dane zabezpieczane są również przez prawa dostępu, pozwalające na dostęp do określonych części sieci tylko niektórym grupom użytkowników.
12. Dla zapewnienia ochrony danych przed wirusami, czy też awarią sprzętu należy często przygotowywać kopie zapasowe danych na CD
13. Przed wirusami chronią programy antywirusowe, które należy aktualizować dwa razy w tygodniu.
14. Mechanizm zabezpieczające przed atakami to działanie służące do wykrywania, zapobiegania

i likwidowania skutków ataku. Możemy rozróżnić następujące mechanizmy zabezpieczające:

- szyfrowanie wiadomości (kryptografia)
- uwierzytelnianie informacji (podpisy cyfrowe)
- ochrona antywirusowa (oprogramowanie antywirusowe)
- identyfikacja i uwierzytelniane osób uprawnionych (hasła i loginy)

15. Przed zagrożeniami fizycznymi tj. brakiem prądu, przepięciami stosuje się zasilacze awaryjne UPS'y, listwy przeciwprzepięciowe.
16. System ochrony dowodów księgowych i innych dokumentów stanowi system zabezpieczeń fizycznych, na które składają się:
    - drzwi z zamontowanymi zamkami,
    - szafy drewniane i kartotekowe z zamkami
17. Dowody księgowe i dokumenty inwentaryzacyjne przechowuje się w siedzibie jednostki w oryginalnej postaci, w ustalonym porządku dostosowanym do sposobu prowadzenia ksiąg rachunkowych, w podziale na okresy sprawozdawcze, w sposób pozwalający na ich łatwe odszukanie. Roczne zbiory dowodów księgowych i dokumentów inwentaryzacyjnych oznacza się określeniem nazwy ich rodzaju oraz symbolem końcowych lat i końcowych numerów w zbiorze.
18. Z wyłączeniem dokumentów dotyczących przeniesienia praw majątkowych do nieruchomości, list płac, powierzenia odpowiedzialności za składniki aktywów, znaczących umów i innych ważnych dokumentów określonych przez Dyrektora, po zatwierdzeniu sprawozdania finansowego treść dowodów księgowych może być przeniesiona na nośniki danych, pozwalające zachować w trwałej postaci zawartość dowodów. Warunkiem stosowania tej metody przechowywania danych jest posiadanie urządzeń pozwalających na odtworzenie dowodów w postaci wydruku, o ile inne przepisy nie stanowią inaczej.
19. Po zatwierdzeniu sprawozdania finansowego za dany rok obrotowy, dokumentację przyjętych zasad rachunkowości, księgi rachunkowe oraz sprawozdania finansowe, w tym również sprawozdanie z działalności jednostki, przechowuje się w archiwum jednostki.
20. Udostępnienie osobie trzeciej zbiorów lub ich części:
    - do wglądu na terenie jednostki - wymaga zgody Dyrektora lub jego zastępcy
    - poza siedzibą zarządu (oddziału) jednostki - wymaga pisemnej zgody Dyrektora oraz pozostawienia w jednostce potwierdzonego spisu przejętych dokumentów, chyba że odrębne przepisy stanowią inaczej.