Załącznik Nr 4
do Zarządzenia Nr 46/2006 Starosty Pułtuskiego
z dnia 2 listopada 2006r.

ZASADY OCHRONY DANYCH I ICH ZBIORÓW GENEROWANE Z KOMPUTEROWYCH PROGRAMÓW PRZETWARZANIA

Przetwarzane dane w systemie FK Budżet podlegają szczegółowej ochronie ze względu na możliwość:

- całkowitej utraty danych ,
- częściowej utraty danych,
- uszkodzeniu danych podczas przetwarzania,
- celowego wprowadzenia błędnych danych przez osoby nieuprawnione,
- wejścia w posiadanie danych przez osoby nieuprawnione.

Mając na względzie powyższe zagrożenia , ustala się co następuje :

1) obowiązek sporządzania zapasowych kopii danych za pomocą znajdującego się w programie FK Budżet oprogramowania Pakiet dla Administracji – INFO-SYSTEM programu archiwizującego na dyskietkach 3,5, płycie CD oraz równolegle na partycji D dysku twardego komputera stacjonarnego
2) wprowadza się obowiązek sporządzania kopii zapasowej , co należy dokonywać przy każdorazowym wprowadzaniu danych do komputera,
3) wprowadza się obowiązek sporządzenia kopii zapasowej , co spoczywa na operatorze , który jako ostatni w danym dniu pracował z systemem ; odpowiedzialność za prawidłową realizację tego obowiązku spoczywa na Skarbniku – Głównym Księgowym – jako osobie odpowiedzialnej za prowadzenie ksiąg rachunkowych w Starostwie.
4) Dyskietki i płyty zawierające dane muszą być przechowywane , do czasu ponownego wykorzystania , pod zamknięciem: wskazane jest przechowywanie ich w innym pomieszczeniu niż znajduje się komputer zawierający dane.
5) Dyskietki i płyty zawierające dane zarchiwizowane w ostatnim dniu roboczym tygodnia mogą zostać powtórnie wykorzystane , nie wcześniej niż po zakończeniu miesiąca.
6) Dyskietki, płyty zawierające dane zarchiwizowane w dniu zamknięcia kolejnego miesiąca i sporządzeniu wydruków , powinny być przechowywane, co najmniej do dnia ostatecznego zatwierdzenia sprawozdania finansowego za dany rok obrotowy: przechowuje się je bezwzględnie pod zamknięciem w innym pomieszczeniu niż znajduje się komputer zawierający dane, w miarę możliwości należy je przechowywać w odpowiednio zabezpieczonym miejscu .
7) Do płyt instalacyjnych programów oraz ich kopii zapasowych stosuje się odpowiednio postanowienia punktu 6.

Wprowadza się następujące zasady ochrony danych przed możliwością całkowitej lub częściowej ich utraty w wyniku różnych zdarzeń, a w szczególności:

1) od kradzieży sprzętu komputerowego; pomieszczenie w którym znajduje się komputer zawierający chronione dane , musi być zamykane w okresie gdy nie przebywa w nim żaden z pracowników, oraz odpowiednio zabezpieczone przed możliwością włamania.
2) Od całkowitego zniszczenia sprzętu komputerowego w wyniku pożaru , zalania lub innych zdarzeń losowych: przechowywanie zapasowych kopii danych i programu instalacyjnego powinno być zgodne z wyżej ustalonymi, zasadami,: obowiązuje też zapewnienie nadzoru nad pomieszczeniem poza godzinami pracy.
3) Od uszkodzenia sprzętu komputerowego spowodowanego niewłaściwymi parametrami zasilania z sieci energetycznej: wymagane jest zapewnienie właściwego stanu instalacji zasilającej, stosowanie wyłącznie instalacji z uziemieniem oraz zasilaczy awaryjnych (tak zwanych UPS) lub co najmniej urządzeń zapewniających eliminację przepięć występujących w sieci energetycznej,
4) Od świadomego usunięcia danych z twardego dysku : obowiązuje maksymalne ograniczenie dostępu do komputera zawierającego dane księgowe, a także bezwzględny zakaz pozostawiania włączonego komputera(lub terminalu) w sieci bez opieki lub możliwości uruchomienia programu oraz dokonywania w nim jakiejkolwiek operacji z klawiatury bez podania hasła ,
5) Od przypadkowego usunięcia danych przez użytkownika: obowiązuje szczególna uwaga przy wykonywaniu operacji usuwających zbiory (kasowanie , formatowanie),

6) Od przypadkowego usunięcia lub ,modyfikacji danych w wyniku działania innego programu (wirusa) : obowiązuje bezwzględny zakaz wykorzystywania komputera do odtwarzania danych i uruchamiania programów z jakichkolwiek nośników nie poddanych uprzednio sprawdzeniu programem antywirusowym i bezpośrednich połączeń z rozległymi sieciami.

Ochrona danych przed uszkodzeniem w trakcie przetwarzania danych powinna być zapewniona przez stosowanie przetestowanego uprzednio sprzętu i właściwych parametrów zasilania.

Ochrona danych przed celowym ich zniekształceniem przez osoby niepowołane polega na przestrzeganiu powyższych ustaleń zawartych w pkt. 4 oraz zdefiniowaniu dla każdego użytkownika programu księgowego jego identyfikatora i hasła. W przypadku używania komputera w sieci lokalnej, administrator sieci obowiązany jest dodatkowo ograniczyć dostęp do katalogów z programami księgowymi wyłącznie dla użytkowników uprawnionych.

Ochrona przed wejściem w posiadanie danych przez osoby nieuprawnione polega na::

1) przestrzeganiu postanowień dotyczących fizycznego ograniczenia dostępności sprzętu,
2) przestrzeganiu postanowień dotyczących zabezpieczeń programowych (definicji haseł użytkowników , przestrzegania zachowania poufności haseł),
3) ograniczeniu do niezbędnego minimum możliwości zdalnej pracy (spoza siedziby Urzędu) na komputerze zawierającym dane księgowe,
4) bezwzględnym przestrzeganiu zasad przechowywania kopii archiwalnych,

Zapewnienie prawidłowych zasad systemu bezpieczeństwa danych polega na :

1) wyznaczeniu jednego administratora odpowiedzialnego za nadawanie określonych uprawnień pozostałym operatorom programów,
2) posiadaniu przez wszystkich użytkowników programów identyfikatora elektronicznego i hasła umożliwiających rozpoznanie zapisów dokonywanych przez te osoby.

Wyznaczenie administratorów sieci oraz dopuszczenie innych osób do danych księgowych w systemie oprogramowania , a także do kontrolowania przez te osoby postanowień ustalonych w tej części przyjętych zasad (polityki) rachunkowości należy do obowiązków Skarbnika – Gł. Księgowego.