

## **Instrukcja w sprawie zasad ochrony i archiwizacji zbiorów danych księgowych i nośników informacji w systemie komputerowym F-K**

### **1. Przedmiot i zakres stosowania instrukcji.**

- 1) Przedmiotem niniejszej instrukcji są zasady zabezpieczenia i ochrony danych księgowych, zbioru danych, programów i nośników magnetycznych stosowanych w eksploatacji systemu informatycznego F-K i podsystemów współpracujących z tym systemem.
- 2) Ustalone w tej instrukcji zasady obowiązują wszystkich użytkowników systemu F-K i podsystemów współpracujących z systemem rachunkowości Urzędu wspomaganych za pomocą komputerów.
- 3) Reguły instrukcji obejmują również procedury w zakresie archiwizowania ksiąg rachunkowych, sprawozdań finansowych programów i danych systemu informacyjnego rachunkowości.

### **2. Zasady ochrony danych, ich zbiorów, programów i nośników informacji w systemie komputerowym F-K.**

- 1) Ze względu na szereg zagrożeń w przetwarzaniu danych księgowych za pomocą komputera uzyskane dane, ich zbiory, programy i nośniki danych podlegają szczególnej ochronie, z uwagi na możliwości:
  - całkowitej utraty danych,
  - częściowej utraty danych,
  - uszkodzenia danych podczas przetwarzania,
  - celowego wprowadzenia błędnych danych przez osoby nieuprawnione,
  - wejścia w posiadanie danych przez osoby nieuprawnione,
  - różnych innych zagrożeń.
- 2) W celu zapobieżenia istniejącym zagrożeniom wprowadza się następujące zasady:
  1. wprowadza się obowiązek sporządzania zapasowych kopii danych przy pomocy programu archiwizującego w oparciu o dedykowane rozwiązania techniczne służące archiwizacji i zabezpieczeniu danych,
  2. wprowadza się obowiązek sporządzania kopii zapasowych co należy wykonywać w ustalonym cyklu,
  3. wprowadza się obowiązek sporządzania kopii zapasowych przez osoby odpowiedzialne i wyznaczone dla tych czynności,
  4. nośniki zawierające zarchiwizowane dane muszą być przechowywane do czasu ponownego wykorzystania po zamknięciu, oraz przechowywane w innym pomieszczeniu niż znajduje się komputer zawierający dane,
  5. nośniki zawierające dane zarchiwizowane w ostatnim dniu roboczny tygodnia, mogą zostać powtórnie wykorzystane, nie wcześniej niż po zakończeniu miesiąca. Nośniki te przechowuje się w zamkniętym innym pomieszczeniu niż znajduje się komputer zawierający dane,
  6. nośniki zawierające dane zarchiwizowane przechowuje się pod zamknięciem w innym pomieszczeniu niż znajduje się komputer zawierający dane, i należy je przechowywać w odpowiednio zabezpieczonym miejscu poza siedzibą Urzędu, a przynajmniej w oddalonym pomieszczeniu.

- 3) W celu ochrony danych i ich zbiorów przed możliwością ich całkowitej lub częściowej utraty w wyniku różnych nieprzewidzianych zdarzeń wprowadza się poniższe zasady:
1. od kradzieży sprzętu komputerowego, pomieszczenie, w którym znajduje się komputer zawierający dane chronione, 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 winno być zgodne w wyżej ustalonymi zasadami, a poza godzinami pracy Urzędu, winien być zapewniony nadzór nad pomieszczeniami Urzędu,
  3. od uszkodzenia sprzętu komputerowego spowodowanego niewłaściwymi parametrami zasilania sieci energetycznej, wymagane jest zapewnienie właściwego stanu instalacji zasilającej, stosowanie wyłącznie instalacji z uziemieniem oraz zasilaczy awaryjnych 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 zakaz pozostawiania włączonego komputera w sieci bez opieki lub możliwości uruchamiania programu oraz dokonywania w nim jakiejkolwiek operacji z klawiatury bez hasła dostępu,
  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 zakaz wykorzystywania komputera do odtwarzania danych i uruchamiania programów z jakichkolwiek nośników nie poddanych uprzednio sprawdzeniu programem antywirusowym i bezpośrednich połączeń z rozległymi sieciami,
- 4) Ochrona danych przed uszkodzeniem w trakcie przetwarzania powinna być zapewnienia przez stosowanie przetestowanego uprzednio sprzętu i właściwych parametrów zasilania.
- 5) Ochrona danych przed celowym ich zniekształceniem przez osoby niepowołane, polega na przestrzeganiu powyższych ustaleń oraz zdefiniowaniu dla każdego użytkownika komputera w sieci lokalnej, administrator sieci obowiązany jest dodatkowo ograniczyć dostęp do katalogów z programem księgowym wyłącznie do użytkowników uprawnionych.
- 6) Ochrona przez wejściem w posiadanie danych przez osoby nieuprawnione polega na:
1. przestrzeganiu postanowień dotyczących fizycznego ograniczenia dostępności sprzętu,
  2. przestrzeganiu postanowień dotyczących zabezpieczeń programowych – definicji użytkowników haseł, przestrzeganiu zachowania poufności haseł,
  3. ograniczeniu do niezbędnego minimum możliwości zdalnej pracy (spoza siedziby Urzędu) na komputerze zawierającym dane księgowe,
  4. przestrzeganiu zasad przechowywania kopii archiwalnych.
- 7) Zapewnienie prawidłowych zasad systemu bezpieczeństwa danych polega na:
1. wyznaczeniu administratora lub administratorów odpowiedzialnych za nadawanie określonych uprawnień pozostałym operatorom programu,

- posiadaniu przez wszystkich użytkowników programu identyfikatora elektronicznego i hasła umożliwiających rozpoznanie zapisów dokonywanych przez te osoby.
- 8) Wyznaczenie administratorów sieci oraz dopuszczenie innych osób do danych księgowych w systemie oprogramowania a także do kontrolowania przestrzegania przez te osoby postanowień ustalonych i przyjętych zasad (polityki) rachunkowości należy do Skarbnika Gminy.
- 9) Przy prowadzeniu rachunkowości za pomocą komputerów system ochrony danych polega na:
- stosowaniu odpornych za zagrożenia nośników danych oraz środków ich zewnętrznej ochrony,
  - systematycznym tworzeniu rezerwowych kopii zbiorów danych zarejestrowanych
  - na nośnikach komputerowych z uwzględnieniem zapewnienia trwałości zapisów,
  - zapewnieniu ochrony programów komputerowych i danych informatycznego systemu rachunkowości, na zasadzie stosowania właściwych rozwiązań organizacyjnych i programowych stanowiących ochronę przed nieupoważnionym dostępem lub zniszczeniem.
- 10) Przy prowadzeniu ksiąg rachunkowych przy użyciu komputerów za równoważne z nimi uznaje się informatyczne zasoby rachunkowości zorganizowane w formie oddzielnych zbiorów danych, baz danych lub ich wyodrębnionych części bez względu na miejsce powstania i przechowywania. Umożliwia to posiadane przez Urząd oprogramowania pozwalającego na uzyskanie czytelnych informacji dotyczących zapisów w księgach rachunkowych poprzez ich wydrukowanie lub przeniesienie na inny nośnik danych o co należy zadbać. W przypadku gdy system ochrony zbiorów danych ksiąg rachunkowych na nośnikach komputerowych nie spełnia w pełni warunków ich ochrony, to zapisy dokonane na komputerowych nośnikach danych powinny być wydrukowane najpóźniej na koniec roku obrotowego. Przeniesienie i przechowywanie zapisów ksiąg rachunkowych na inny nośnik danych dopuszcza się pod warunkiem zapewnienia możliwości ich odtworzenia w formie wydruków.
- 11) Księgi rachunkowe mogą mieć formę zbiorów utwalonych na komputerowych nośnikach danych pod warunkiem przestrzegania zasad ich ochrony jeżeli są, podobnie prowadzone jak w formie tradycyjnej:
- trwale oznaczone nazwą Gminy, nazwą danego rodzaju księgi (zbioru) oraz nazwą programu przetwarzania,
  - starannie przechowywane z góry ustalonej kolejności.