Zasady ochrony danych

Przetwarzane dane w systemie komputerowym podlegają szczególnej ochronie ze względu na możliwość:

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

Mając na względzie powyższe zagrożenia wprowadza się obowiązek codziennej archiwizacji danych. Kopie zapasowe dysków twardych posiadające dane osobowe oraz niezbędne dane potrzebne do pracy na Cmentarzu Komunalnym robione są codziennie. Na serwerze działają skrypty robiące kopie komputerów każdego dnia o godzinie 23^{00}. Ponadto 3 razy w tygodniu dane kopiowane są na inny komputerowy nośnik danych w celach bezpieczeństwa. Komputery posiadające dane osobowe nie są podłączone do Internetu.

Baza archiwalna tworzona jest automatycznie na serwerze każdego dnia. Raz na miesiąc dane tygodniowe przenoszone są na komputerowe nośniki danych.

1. Nośniki zawierające zarchiwizowane dane należy przechowywać pod zamknięciem. Wskazane jest przechowywanie ich w innym pomieszczeniu niż znajduje się komputer zawierający dane,
2. Nośniki zawierające dane zarchiwizowane, skopiowane w dniu zamknięcia kolejnego miesiąca, przechowuje się, co najmniej do dnia ostatecznego zatwierdzenia sprawozdania finansowego za dany rok obrotowy. Na koniec roku obrotowego przenosi się treść ksiąg rachunkowych na komputerowy nośnik danych, zapewniający trwałość zapisu informacji, i przechowuje przez czas nie krótszy od wymaganego dla przechowywania ksiąg rachunkowych. Nośniki te przechowuje się bezwzględnie pod zamknięciem w innym pomieszczeniu niż znajduje się komputer zawierający dane; w miarę możliwości należy je przechowywać w odpowiednio zabezpieczonym miejscu,
3. Do płyt instalacyjnych programu oraz ich kopii zapasowych stosują się odpowiednio postanowienia punktu 6 zasad ochrony danych.

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 pomieszczeniami Cmentarza Komunalnego 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. Na Cmentarzu Komunalnym w Częstochowie każda workstation posiada lokalny UPS.
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 jakiekolwiek 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.
Na Cmentarzu Komunalnym w Częstochowie wszystkie bazy danych posiadające dane osobowe są chronione hasłami. Programy, które posiadają okresowe hasło oraz blokowanie po błędnym wpisaniu to: Płatnik 7.02.001 oraz Wilksoft Kameleon SQL. Programy, które są chronione hasłem to Biznesmen Kadry Płace i ZUS 4.15.82.
Na Cmentarzu Komunalnym w Częstochowie wdrożony jest system logowania do domeny (Samba) to serwer zarządza nadawaniem praw oraz zasobów użytkownikom. Podczas logowania mapowane są również dyski sieciowe oczywiście wszystko jest kontrolowane przez administratora.
Program Księgowy Kameleon SQL posiada możliwość konfigurowania dostępu użytkowników, nadawaniu im odpowiednich uprawnień.
Ochrona danych przed uszkodzeniem w trakcie przetwarzania 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 punkcie 4 oraz zdefiniowaniu dla każdego użytkownika programu księgowego jego identyfikatora i hasła. Administrator sieci w porozumieniu z Dyrektorem zakładu dodatkowo ogranicza dostęp do katalogów z programem księgowym wyłącznie do użytkowników uprawnionych.

Ochrona przed wejściem w posiadanie danych przez osoby nieuprawnione polega na:
przestrzeganiu postanowień dotyczących fizycznego ograniczenia dostępności sprzętu,
przestrzeganiu postanowień dotyczących zabezpieczeń programowych (definicji użytkowników haseł, przestrzegania zachowania poufności haseł), systemie haseł, których okresowa zmiana wymuszana jest przez system niezależnie od blokowania dostępu po 3-krotnym błędnym wpisaniu hasła,
kontroli grupy, do której musi należeć użytkownik, by w czasie logowania system przydzielił odpowiednie zasoby i zmapował dyski sieciowe,
nadawaniu dostępu do aplikacji poprzez system uprawnień (uprawnienia dotyczą nie tylko możliwości uruchomienia samej aplikacje, lecz także – niezależnie - poszczególnych jej funkcji).
bezwzględnym przestrzeganiu zasad przechowywania kopii archiwalnych.

Zapewnienie prawidłowych zasad sytemu bezpieczeństwa danych polega na:
wyznaczeniu jednego administratora odpowiedzialnego za nadawanie określonych uprawnień pozostałym operatorom programu,
posiadaniu przez wszystkich użytkowników programu 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 przestrzegania przez te osoby postanowień ustalonych w tej części przyjętych zasad (polityki) rachunkowości należy do obowiązków głównego księgowego lub do osoby prowadzącej księgi rachunkowe.