Załącznik Nr 4
do Zarządzenia nr 45A/2010
Wójta Gminy Kowiesy
z dnia 25 października 2010 r.

Instrukcja określająca system ochrony danych w Urzędzie Gminy Kowiesy

CZĘŚĆ I

Sposób zarządzania systemem informatycznym

§ 1

Zarządzanie systemami haseł

1. Osobą odpowiedzialną za sposób przydziału haseł dla użytkowników oraz częstotliwość ich zmiany jest informatyk.
2. Każdy użytkownik systemu informacyjnego ma okresowo zmieniane hasło dostępu.
3. Dostęp do zasobów systemów odbywać się może tylko w oparciu o system haseł przydzielanych indywidualnie dla pracowników oraz użytkowników systemu.
4. Zapewnione jest generowanie haseł w cyklu miesięcznym. Użytkownicy mają obowiązek zmieniać swoje hasło nie rzadziej niż co 30 dni.
5. Użytkownik nie może udostępniać swego hasła innym osobom.
6. Przekazywanie haseł odbywa się w sposób poufny i nie może ono być zapisywane w miejscu pozwalającym na dostęp dla osób nieupoważnionych.
7. W przypadku utraty hasła lub istnienia podejrzenia naruszenia systemu haseł przez osoby nieuprawnione, dotychczasowy zestaw haseł musi być niezwłocznie unieważniony i zastąpiony nowym.

§ 2

Zasady rejestrowania i wyrejestrowywania użytkowników.

1. Osobą odpowiedzialną za rejestrowanie i wyrejestrowywanie użytkowników w jednostce jest informatyk.
2. Podstawą do zarejestrowania użytkownika do danego systemu przetwarzania danych jest zakres czynności pracownika. Natomiast podstawą do wyrejestrowania użytkownika z danego systemu przetwarzania danych jest nowy zakres czynności pracownika lub jego zwolnienie.
3. Administrator rejestruje oraz wyrejestrowuje użytkowników, przy przetwarzaniu danych archiwizując imię i nazwisko użytkownika.
4. Osoby dopuszczone do przetwarzania danych zobowiązane są do zachowania tajemnicy (dostępu do danych i ich merytorycznej treści). Obowiązek ten istnieje również po ustaniu zatrudnienia.

§ 3.

Procedury rozpoczęcia i zakończenia pracy.

1. Użytkownicy przed przystąpieniem do pracy przy przetwarzaniu danych powinni zwrócić uwagę, czy nie istnieją przesłanki do tego, że dane zostały naruszone.

2. Dostęp do konkretnych zasobów danych jest możliwy dopiero po podaniu właściwego identyfikatora i hasła dostępu.

3. Hasło użytkownika należy podawać do systemu w sposób dyskretny (nie literować, nie czytać na głos, wpisywać osobiście, nie pozwalać na bezpośrednią obecność drugiej osoby podczas wpisywania hasła, itp.).

4. Użytkownik ma obowiązek zamykania systemu, programu komputerowego po zakończeniu pracy. Stanowisko komputerowe z uruchomionym systemem, programem nie może pozostawać bez kontroli pracującego na nim użytkownika.

§ 4.

Obsługa kopii bezpieczeństwa, nośników informacji oraz wydruków.

1. Wydruki z systemów informatycznych oraz inne nośniki informacji muszą być zabezpieczone w sposób uniemożliwiający do nich dostęp przez osoby nieupoważnione w każdym momencie przetwarzania, a po upływie czasu ich przydatności są niszczone lub archiwizowane w zależności od kategorii archiwalnej.

2. Wydruki, maszynowe nośniki informacji (dyskietki, dyski optyczne, itp.) oraz inne dokumenty, zawierające dane przeznaczone do likwidacji, muszą być pozbawione zapisów lub w przypadku gdy jest to możliwe, muszą być trwale uszkodzone w sposób uniemożliwiający odczytanie z nich informacji.

3. Urządzenia, dyski i inne informatyczne nośniki danych (np. dyskietki) zawierające dane przed ich przekazaniem innemu podmiotowi, winny być pozbawione zawartości. Naprawa wymienionych urządzeń zawierających dane, jeżeli nie można danych usunąć, winna być wykonywana pod nadzorem osoby upoważnionej.

4. Administrator wykonuje raz na tydzień podwójną kopię wszystkich danych na dyskach optycznych.

Część II
Ochrona danych

§ 5.

Ochrona danych przed ich utratą z systemów informatycznych.

1. Urządzenia i systemy informatyczne zasilane energią elektryczną powinny być zabezpieczone przed utratą danych, spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej (zasilacze awaryjne UPS).

2. Włamanie do pomieszczeń, w których przetwarza się dane powinno być uniemożliwione poprzez zabezpieczenie okien i drzwi wejściowych.

3. Pomieszczenia komputerowe powinny być zabezpieczone przed pożarem.

4. Instalacja oprogramowania może odbywać się tylko przez administratora lub pod jego nadzorem.

5. W celu ochrony przed wirusami komputerowymi, używanie nośników danych (np. dyskietki, dyski optyczne, itp.) spoza jednostki jest dopuszczalne dopiero po uprzednim sprawdzeniu ich przez administratora i upewnieniu się, że nośniki te nie są „zarażone" wirusem.

6. W przypadku stwierdzenia obecności wirusów komputerowych w systemie należy postępować zgodnie z „Instrukcją postępowania w sytuacji naruszenia zasad ochrony systemów informatycznych".

§ 6.

Sposób komunikacji w zakresie sieci komputerowej.

1. Dopuszcza się łączenie z siecią internetu i używanie poczty elektronicznej tylko na zestawach komputerowych, wyposażonych w zabezpieczenia antywirusowe.

2. Przesyłanie danych na nośnikach zewnętrznych (np. dyskietki, wydruki) na zewnątrz jednostki może odbywać się tylko w formie przesyłki poleconej. Zabrania się przekazywania danych w jawnej formie za pośrednictwem internetu (poczty elektronicznej).

§ 7.

Przeglądy i konserwacja systemów i zbiorów danych.

1. Przeglądów i konserwacji systemów przetwarzania danych dokonuje administrator bezpieczeństwa informacji co najmniej raz w miesiącu.

2. Ocenie podlegają stan techniczny urządzeń (komputery, serwery, UPS-y, itp.), stan okablowania budynku w sieć logiczną, spójność baz danych, stan zabezpieczeń fizycznych (zamki, kraty), stan rejestrów systemów serwera lokalnej sieci komputerowej.

§ 8.

Postępowanie w sytuacjach naruszenia zasad ochrony systemów informatycznych.

1. Możliwe sytuacje świadczące o naruszeniu zasad ochrony danych przetwarzanych w systemie informatycznym.

Każde domniemanie, przesłanka, fakt wskazujący na naruszenie zasad ochrony danych, a zwłaszcza stan różny od ustalonego w systemie informatycznym, w tym:

1) stan urządzeń (np. brak zasilania, problemy z uruchomieniem),
2) stan systemu zabezpieczeń obiektu,
3) stan aktywnych urządzeń sieciowych i pozostałej infrastruktury informatycznej,
4) zawartość zbioru danych (np. brak lub nadmiar danych),
5) ujawnione metody pracy,
6) sposób działania programu (np. komunikaty informujące o błędach, brak dostępu do funkcji programu, nieprawidłowości w wykonywanych operacjach),
7) przebywanie osób nieuprawnionych w obszarze przetwarzania danych,
8) inne zdarzenia mogące mieć wpływ na naruszenie systemu informatycznego (np. obecność wirusów komputerowych)

– stanowi dla osoby uprawnionej do przetwarzania danych, podstawę do natychmiastowego działania.

2. Sposób postępowania.

1) O każdej sytuacji odbiegającej od normy, a w szczególności o przesłankach naruszenia zasad ochrony danych w systemie informatycznym, opisanych w pkt. 1, należy:
   – natychmiast informować administratora lub osobę przez niego upoważnioną,
   – niezwłocznie taką sytuację zarejestrować w dzienniku pracy właściwym dla stanowisk, na którym to zdarzenie miało miejsce.
2) Osoba stwierdzająca naruszenie przepisów lub stan mogący mieć wpływ na bezpieczeństwo, zobowiązana jest do możliwie pełnego udokumentowania zdarzenia, celem precyzyjnego określenia przyczyn i ewentualnych skutków naruszenia obowiązujących zasad.
3) Stwierdzone przez administratora naruszenie zasad ochrony danych osobowych wymaga powiadomienia kierownika jednostki oraz natychmiastowej reakcji poprzez:
   – usunięcie uchybień (np. wymiana niesprawnego zasilacza awaryjnego, usunięcie wirusów komputerowych z systemu, itp.),
   – zastosowanie dodatkowych środków zabezpieczających zgromadzone dane,
   – wstrzymanie przetwarzania danych do czasu usunięcia awarii systemu informatycznego.

Część III

Przechowywanie zbiorów

§ 9

1. Kompletne księgi rachunkowe drukowane są nie później niż na koniec roku obrotowego. Za równoważne z wydrukiem uznaje się przeniesienie treści ksiąg rachunkowych na inny komputerowy nośnik danych, zapewniający trwałość zapisu informacji, przez czas nie krótszy niż 5 lat.

2.W sposób trwały (nie krótszy niż 50 lat) przechowywane są zatwierdzone sprawozdania finansowe, a także dokumentacja płacowa (listy płac, karty wynagrodzeń albo inne dowody, na podstawie których następuje ustalenie podstawy wymiaru emerytury lub renty), licząc od dnia, w którym pracownik przestał pracować u danego płatnika składek na ubezpieczenia społeczne (art. 125a ust. 4 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z FUS (tekst jednolity Dz. U. z 2004 r. Nr 39, póz. 353 z późn. zm.).

3. Okresowemu przechowywaniu podlegają:
- dowody księgowe dotyczące pożyczek, kredytów i innych umów, roszczeń dochodzonych w postępowaniu cywilnym, karnym i podatkowym - przez 5 lat od początku roku następującego po roku obrotowym, w którym operacje, transakcje i postępowanie zostały ostatecznie zakończone, spłacone, rozliczone lub przedawnione,
- dokumentacja przyjętego sposobu prowadzenia rachunkowości - przez okres nie krótszy niż 5 lat od upływu ich ważności,
- dokumenty dotyczące rękojmi i reklamacji - 1 rok po terminie upływu rękojmi lub rozliczeniu reklamacji,
- księgi rachunkowe, dokumenty inwentaryzacyjne oraz pozostałe dowody księgowe i dokumenty - przez okres 5 lat.

Powyższe terminy oblicza się od początku roku następującego po roku obrotowym, którego dane zbiory (dokumenty) dotyczą.

4. Udostępnianie danych i dokumentów

Udostępnienie sprawozdań finansowych i budżetowych oraz dowodów księgowych, ksiąg rachunkowych i innych dokumentów z zakresu rachunkowości jednostki ma miejsce:

- w siedzibie jednostki po uzyskaniu zgody kierownika jednostki lub upoważnionej przez niego osoby,
- poza siedzibą jednostki po uzyskaniu pisemnej zgody kierownika jednostki i pozostawieniu pisemnego pokwitowania zawierającego spis wydanych dokumentów.

WÓJT GMINY

mgr inż. Andrzej Józef Luboiński