Zarządzenie Nr 42/04
Wójta Gminy Stolno
z dnia 29 listopada 2004 roku

w/s instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Na podstawie art. 36 ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. z 2002 roku Nr 101, poz. 926 ze zm.) oraz na podstawie § 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w/s dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024)

zarządzam, co następuje:

§ 1
Wprowadzam do stosowania w Urzędzie Gminy Stolno, Gminnej Bibliotece Publicznej w Stolnie oraz w Gminnym Zespole Komunalnym w Stolnie instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, stanowiącą załącznik do niniejszego zarządzenia.

§ 2
Wyznaczam na administratora bezpieczeństwa informacji Pana Janusza Frąckiewicza.

§ 3
Zarządzenie wchodzi w życie z dniem podjęcia.

§ 4
Traci moc instrukcja zarządzania systemem informatycznym służącym przetwarzaniu danych osobowych z 25 października 1999 roku.

WÓJT
mgr inż. Jerzy Rabeszko

Załącznik
do Zarządzenia Nr 42/04
z dnia 29 listopada 2004 roku

INSTRUKCJA
W SPRAWIE ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM PRZETWARZANIU DANYCH OSOBOWYCH

Zasady ogólne

§ 1

Obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego obejmuje pomieszczenia znajdujące się w budynku Urzędu Gminy Stolno i są to pokoje o numerach: 14, 16, 17 i 20 oraz pomieszczenie nr 5, w którym przetwarzane są dane osobowe bez użycia komputerów.

§ 2

Wewnątrz obszaru, o którym mowa w § 1, osoby nieuprawnione do dostępu do danych osobowych mogą przebywać wyłącznie w obecności osoby upoważnionej do przetwarzania tych danych i za zgodą administratora danych lub osoby przez niego upoważnionej.

§ 3

Pomieszczenia, w których przetwarzane są dane osobowe, na czas nieobecności w nich osób upoważnionych do przetwarzania danych muszą być zamykane w sposób uniemożliwiający dostęp do nich osób postronnych. Urządzenia i systemy informatyczne służące przetwarzaniu danych zasilane energią elektryczną muszą być, przez cały czas zabezpieczone przed utratą tych danych spowodowaną awarią zasilania lub zakłóceniami sieci zasilającej.

§ 4

Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych, mogą być dopuszczone wyłącznie osoby posiadające upoważnienie wydane przez administratora danych lub osobę przez niego upoważnioną.

Zarządzanie systemem informatycznym

§ 5

1. Wszyscy użytkownicy korzystający z systemu informatycznego zobowiązani są do posługiwania się przydzielonymi hasłami zmienianymi co miesiąc oraz identyfikatorami, które nie powinny być zmieniane, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinny być przydzielone innym osobom.
2. Hasła oraz identyfikatory ustala administrator bezpieczeństwa informacji.

3. Przydział pierwszego hasła dokonuje administrator bezpieczeństwa informacji, następnych zmian hasła dokonuje osoba upoważniona do przetwarzania danych i zgłasza zmianę administratorowi bezpieczeństwa informacji.
4. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych, należy niezwłocznie wyrejestrować, unieważnić jej hasło oraz podjąć inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych.
5. Administrator bezpieczeństwa informacji wykonuje niezbędne czynności związane z zapewnieniem integralności danych, sposobu ich rozmieszczania na nośnikach (dokonywanie defragmentacji).

§ 6

Użytkownicy korzystający z systemu są zarejestrowani i wyrejestrowywani przez administratora bezpieczeństwa informacji poprzez wpisanie lub wykreślenie z rejestru.

§ 7

Użytkownicy przystępując do pracy powinni podać hasło dostępu do komputera i do używanej aplikacji, zaś kończąc pracę zakończyć program, wyłączyć komputer i ewentualnie drukarkę.

§ 8

1. Użytkownicy zobowiązani są tworzyć, co tydzień kopie awaryjne, sprawdzając równocześnie, co miesiąc, pod kątem ich dalszej przydatności, do odtwarzania danych w przypadku awarii systemu. Po ustaniu użyteczności kopii awaryjnych powinny być one bezzwłocznie usuwane.
2. Użytkownicy przechowują wydruki z danymi osobowymi zamykane w szafach.

§ 9

Administrator bezpieczeństwa informacji zobowiązany jest raz w miesiącu sprawdzić obecność wirusów komputerowych przy użyciu odpowiedniego programu antywirusowego.

§ 10

1. Przeglądy i konserwacje sprzętu komputerowego dokonywane są, co kwartał przez wyspecjalizowaną firmę pod nadzorem administratora bezpieczeństwa informacji.
2. Przeglądy i konserwacje zbioru danych dokonywane są przez pracowników.
3. Administrator bezpieczeństwa informacji lub osoba upoważniona, w przypadku konieczności oddania sprzętu do naprawy na zewnątrz, usuwa zapisy danych.

§ 11

Dla każdej osoby, której dane są przetwarzane powinny być odnotowane:
1. data pierwszego wprowadzenia danych tej osoby;
2. identyfikator użytkownika wprowadzającego dane;
3. komu, kiedy i w jakim zakresie jej dane zostały udostępnione, jeśli przewidziane jest ich udostępnienie innym podmiotom, chyba że dane te traktuje się, jako dane powszechnie dostępne (rejestry).

§ 12

Ekrany monitorów stanowisk dostępu do danych osobowych, powinny być automatycznie włączane po upływie pięciu minut czasu nieaktywności użytkownika.

§ 13

Nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkownika oraz kontroli dostępu do danych osobowych, w które wyposażony jest system informatyczny przetwarzający dane osobowe, sprawuje administrator bezpieczeństwa informacji.