ZARZĄDZENIE Nr 22/2009
STAROSTY GRUDZIĄDZKIEGO
z dnia 30 października 2009 r.

w sprawie zatwierdzenia „Dokumentu polityki zarządzania bezpieczeństwem informacji w Starostwie Powiatowym w Grudziądzu" oraz „Polityki bezpieczeństwa".

Na podstawie art. 34 ust. 1 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2001 r. Nr 142, poz. 1592 z późn. zm.)

zarządzam, co następuje:

§ 1. Zatwierdza się „Dokument polityki zarządzania bezpieczeństwem informacji w Starostwie Powiatowym w Grudziądzu" stanowiący załącznik nr 1 do zarządzenia oraz „Politykę bezpieczeństwa" stanowiącą załącznik nr 2 do zarządzenia.

§ 2. Zobowiązuje się wydziały Starostwa Powiatowego w Grudziądzu oraz jednostki organizacyjne powiatu do przestrzegania założeń zawartych w załączniku nr 1 i 2 do zarządzenia.

§ 3. Traci moc Zarządzenie Nr 4/2007 Starosty Grudziądzkiego z dnia 5 lutego 2007 r. w sprawie zatwierdzenia „Dokumentu polityki zarządzania bezpieczeństwem informacji w Starostwie Powiatowym w Grudziądzu" oraz „Polityki bezpieczeństwa" wypracowanych przez „Zespół ds. zarządzania bezpieczeństwem informacji" w Starostwie Powiatowym w Grudziądzu.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA
Marek Szczepanowski

Załącznik nr 1
do Zarządzenia Nr 21/2009
Starosty Grudziądzkiego

Dokument polityki zarządzania bezpieczeństwem informacji w Starostwie Powiatowym w Grudziądzu

§1
Wprowadzenie

1. Niniejszy dokument określa ogólne zasady zarządzania systemami informatycznymi w Starostwie Powiatowym w Grudziądzu.

2. Podstawy prawne
1)Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 11, poz. 926 ze zm.)

2) Rozporządzenie MSWiA z dnia 29 kwietnia 2004 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. z 2004 r. Nr 100, poz. 1025).

3) Rozporządzenie MSWiA z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).

4) Normy PN-ISO/IEC 17799 i PN-I-07799-2.

§ 2

Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osób odpowiedzialnych za te czynności.

Zespół ds. zarządzania bezpieczeństwem informacji (Z ds. ZBI) jest odpowiedzialny za bezpieczeństwo danych osobowych w systemie informatycznym Starostwa. Prowadzi rejestr osób upoważnionych do przetwarzania danych osobowych – administratora systemu informatycznego, użytkowników uprzywilejowanych, użytkowników.

§ 3

Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem.

1. Hasła wszystkich użytkowników systemu informatycznego deponowane w formie pisemnej u Z ds. ZBI.

2. Hasło używane do uwierzytelnienia użytkowników ma być zmieniane nie rzadziej niż co 30 dni i musi składać się co najmniej z 8 znaków.

3. Użytkownik jest zobowiązany do zabezpieczenia używanego przez siebie hasła przed użyciem przez osoby nieupoważnione.

4. Zaleca się wykorzystywanie możliwości systemów operacyjnych do zabezpieczeń stacji roboczych wyposażonych w systemy operacyjne o właściwościach podobnych do Windows 2000/XP pod warunkiem zdeponowania identyfikatora i hasła u Z ds. ZBI

5. Stosowanie nie uzgodnionych z Z ds. ZBI sposobów i form zabezpieczenia systemu informatycznego jest zabronione.

§ 4

Procedury rozpoczęcia i zakończenia pracy przeznaczone dla użytkowników systemu.

1. Czynności jakie należy wykonać w celu uruchomienia systemu informatycznego:
   - włączenie źródła zasilania
   - uruchomienie stacji roboczej – zalogowanie się do sieci LAN
   -uruchomienie systemu informatycznego z wykorzystaniem mechanizmów uwierzytelniania wykorzystywanych przez oprogramowanie użytkowe.
   W celu zakończenia pracy z systemem informatycznym należy wykonać powyższe czynności w odwrotnej kolejności.

2. W sytuacji tymczasowego zaprzestania pracy na skutek opuszczenia stanowiska pracy lub w sytuacji, gdy wgląd w wyświetlane na monitorze dane może mieć nieupoważniona osoba należy niezwłocznie przerwać wykonywane operacje i czynności, następnie zakończyć pracę z systemem informatycznym służącym do przetwarzania danych.

3. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego oraz gdy stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać naruszenie zabezpieczeń tych danych należy niezwłocznie podjąć próbę ustalenia ilości utraconych lub przejętych bezprawnie informacji z bazy i poinformować bezpośredniego przełożonego oraz Z. ds. ZBI o stwierdzonym fakcie.

4. Z ds. ZBI uzyskaną informację od pracowników lub Kierowników poddaje analizie w celu ustalenia okoliczności utraty danych zgodnie z obowiązującym stanem prawnym.

5. W przypadku włamania do Starostwa i stwierdzenia naruszenia tajemnicy ochrony danych względnie powzięcia podejrzeń osoba – pracownik, który

stwierdził ten fakt informuje o nim Starostę lub jego Zastępcę oraz Z ds. ZBI, którzy podejmują niezbędne działania zgodnie z niniejszą instrukcją.

§ 5

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

1. Kopie zapasowe danych oraz systemu informatycznego używanego do ich przetwarzania magazynuje Z ds. ZBI.

2. Kopie zapasowe systemu informatycznego używanego do przetwarzania danych wykonuje się nie rzadziej niż raz w miesiącu oraz bezpośrednio przed i po każdej modernizacji i aktualizacji systemu.

3. Kopie zapasowych danych oraz systemu informatycznego używanego do ich przetwarzania zabezpiecza się za pomocą utrwalenia na nośnikach magnetycznych CD.

§ 6

Sposób, miejsce i okres przechowywania kopii zapasowych oraz elektronicznych nośników informacji zawierających dane osobowe.

1. Kopie zapasowe danych oraz systemu informatycznego używanego do ich przetwarzania utrwalone na nośnikach magnetycznych CD należy przechowywać w wydzielonej szafie zabezpieczonej zamkiem.

2. Kopie zapasowe usuwa się niezwłocznie po ustaniu ich użyteczności w sposób uniemożliwiający ich odczytanie.

3. Elektroniczne nośniki informacji wycofane z eksploatacji, a nie przeznaczone do zniszczenia należy pozbawić zawartości w sposób uniemożliwiający odczytanie zapisanych na nich danych.

§ 7

Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.

1. Stacje robocze wykorzystywane do obsługi systemów informatycznych w których przetwarza się dane osobowe narażone są na działalność oprogramowania którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego – wirusy, trojany, keylogery, spyware i inne (WTKS). Szczególnie narażone są komputery wyposażone w stacje dyskietek, czytnik CD lub dostęp do Internetu. Należy wyeliminować możliwość jednoczesnego

korzystania z powyższych rozwiązań technicznych z dostępem do systemów informatycznych służących do przetwarzania danych.

2. Wszyscy użytkownicy systemu informatycznego zobowiązani są do skanowania systemu pod kątem obecności WTKS przed każdorazowym zalogowaniem się do systemów informatycznych służących do przetwarzania danych.

3. Niedozwolone jest indywidualne instalowanie na stanowiskach roboczych oprogramowania niezwiązanego z obsługą systemów informatycznych służących do przetwarzania danych.

§ 8

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

1. Celem wykonywania przeglądów i konserwacji systemów służących do przetwarzania danych jest ich bezawaryjna praca umożliwiająca zachowanie integralności i spójności danych, zapewnienie ich przetwarzania i uzyskiwania w sytuacjach awaryjnych.

2. Przeglądy systemu dokonywane są okresowo przynajmniej raz w tygodniu pod kątem obecności WTKS.

3. W przypadku stwierdzenia awarii systemu, utraty danych, zauważonych przekłamań w bazach danych Z ds. ZBI dokonuje analizy zaistniałej sytuacji awaryjnej, określają przyczynę, przeprowadzają niezbędne czynności w celu wyeliminowania stwierdzonych nieprawidłowości, dokonują niezbędne zmiany w procedurach. Naprawiają system informatyczny na podstawie wykonanej kopii zapasowej zbiorów i systemów.

4. W przypadku wypadku gdy zaistnieje konieczność zlecenia tych czynności osobom nie posiadającym upoważnień do przetwarzania danych wszelkie czynności muszą być wykonywane w obecności Z ds. ZBI.

5. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do naprawy należy pozbawić wcześniej zapisu dych danych w sposób uniemożliwiający ich odzyskanie, bądź też naprawić je pod nadzorem osoby upoważnionej przez Z ds. ZBI.

Załącznik nr 2
do Zarządzenia Nr 21/2009
Starosty Grudziądzkiego

Polityka bezpieczeństwa.

§ 1

Wprowadzenie

1. Politykę bezpieczeństwa należy rozumieć, jako zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych w Starostwie Powiatowym w Grudziądzu.

2. Polityka bezpieczeństwa odnosi się całościowo do problemu zabezpieczenia danych osobowych tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie jak i danych przetwarzanych w systemach informatycznych.

3. Celem polityki bezpieczeństwa, jest wskazanie działań, jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie wykonać obowiązki administratora danych w zakresie zabezpieczenia danych osobowych przy wsparciu osób zatrudnionych w Starostwie.

§ 2

Obszar, w którym przetwarzane są dane osobowe

1. Obszar, w którym przetwarza się dane osobowe stanowi cały budynek położony w Grudziądzu przy ulicy Małomłyńskiej 1 zajmowany przez Starostwo Powiatowe w Grudziądzu (z wyłączeniem pomieszczeń gospodarczych oraz pomieszczeń wynajmowanych innym podmiotom).

2. Przetwarzaniem danych osobowych nazywamy jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

3. Zmiany pomieszczeń wykorzystywanych przez Wydziały Starostwa oraz techniczne możliwości rozwoju sieci, w tym również bezprzewodowej powodują, że praktycznie każde z pomieszczeń Starostwa Powiatowego w Grudziądzu jest wykorzystywane lub może być wykorzystywane do przetwarzania danych osobowych.

§ 3

Wykaz zbiorów danych osobowych prowadzonych w Starostwie Powiatowym w Grudziądzu

Lp.	Komórka organizacyjna Starostwa	Administrator zbioru danych osobowych	Nazwa zbioru danych osobowych	Podstawa prawna przetwarzania danych	System ewidencji i pomieszczenia
1.	**Wydział Organizacyjny**	Agnieszka Zawadka	Rejestr skarg i wniosków	Rozp. RM z 18.12.98 w sprawie instrukcji kancelaryjnej dla organów powiatu	- księga, pok. 22
2.	**Wydział Geodezji, Kartografii, Katastru i Gospodarki Nieruchomościami**	Edward Wiatrowski	Ewidencja osób zgłaszających do zasobu geodezyjnego prace geodezyjne i kartograficzne	art. 12 ust. 2 ustawy z 17.05.89, Prawo geodezyjne i kartograficzne	- komputerowy, pok. 40
			Ewidencja gruntów i budynków	art. 24 ust. 2 z 17.05.89, Prawo geodezyjne i kartograficzne	- komputerowy, pok. 40
			Ewidencja użytkowników wieczystych gruntów stanowiących własność Skarbu Państwa	art. 11 ustawy z dnia 21.08.97 o gospodarce nieruchomościami	- komputerowy, pok. 40
3.	**Wydział Ochrony Środowiska, Leśnictwa, Rolnictwa i Gospodarki Wodnej**	Kazimierz Sobótka	Karty wędkarskie	art. 7 ust. 5 ustawy z 18.04.85 o rybactwie śródlądowym	- komputerowy, pok. 34
			Rejestr łodzi rybackich	art. 20 ust. 1 ustawy 18.04.85 o rybactwie śródlądowym	- komputerowy, pok.34
			Legitymacje Społecznej Straży Rybackiej	art.25 ust. 2 pkt. ustawy z 18.04.85 o rybactwie śródlądowym	- komputerowy, pok. 34
			Plany urządzenia lasów	art. 5 ust. 1 ustawy z 18.04.85 o lasach (Dz.U. z 08.11.91)	- teczka, pok. 34
4.	**Wydział Architektury i Budownictwa**	Henryk Pasik	Rejestr pozwoleń na budowę	Art. 38 ust. 2 ustawy z 07.07.94, Prawo budowlane (Dz.U. 89 poz. 414)	- księga - komputerowy, pok.27
5.	**Wydział Komunikacji**	Andrzej Rodziewicz	Ewidencja instruktorów	Art. 106 ust. 1 ustawy z dnia 20 czerwca 1997 r. Prawo o ruchu drogowym, Dz. U. z 2003 r. Nr 58, poz. 515 z późn. zm.	- kartoteka, pok. 3
			Rejestr kierowców	Art. 100 a ust. 1 ustawy z dnia 20 czerwca 1997 r. Prawo o ruchu drogowym, Dz. U. z 2003 r. Nr 58, poz. 515 z późn. zm.	- komputerowy, - kartoteka, pok. 13

			Rejestr pojazdów	art. 73. Ust. 1 ustawy z dnia 20 czerwca 1997 r. Prawo o ruchu drogowym, Dz. U. z 2003 r. Nr 58, poz. 515 z późn. zm.	- komputerowy, - kartoteka, pok. 4-5
			Ewidencja przedsiębiorstw wykonujących transport krajowy, drogowy oraz na potrzeby własne	Ustawa o transporcie drogowym z 06.09.2001 r.	- katalog, pok. 3
			Rejestr przedsiębiorców prowadzących stacje kontroli pojazdów	art. 83 a, prawo o ruchu drogowym	- kartoteka, pok. 3
			Rejestr przedsiębiorców prowadzących Ośrodki Szkolenia Kierowców	Art. 103, prawo o ruchu drogowym	- kartoteka, pok.3
6.	**Wydział Rozwoju Lokalnego, Edukacji i Zamówień Publicznych**	Dorota Kaczerowska	Rejestr nauczycieli, wychowawców i innych pracowników pedagogicznych ujawnionych w związku z ustawą o systemie informacji oświatowej.	Ustawa z dnia 19.02.2004 r. o systemie informacji oświatowej (Dz. U. Nr 49 poz. 463)	- komputerowy Pok. 33
7.	**Powiatowe Centrum Pomocy Rodzinie**	Jarosław Poznański	Rejestr rodzin zastępczych	art. 78 ust. 1-10 ustawy z dnia 12.03.2004 r. o pomocy społecznej (Dz. U. Nr 64 poz.593) oraz §9, 11 Rozp. MPS z dnia 18.10.2004r. w sprawie rodzin zastępczych (Dz. U. Nr 233, poz. 2344)	- kartoteka, pok. 20
			Rejestr kontynuujących naukę i usamodzielniających się	art.88 ust. O pomocy + §7 Rozp. MpiPS z dnia 9.10.2001 r. (Dz. U. Nr 120, poz. 1293)	- kartoteka, pok. 20
			Rejestr osób niepełnosprawnych, otrzymujących pomoc ze środków PF RON	art.35 a ust.1 ptk. 7 ustawy z dnia 27.08.1997r. o rehabilitacji zawodowej i społecznej oraz zatrudnieniu osób niepełnosprawnych	- kartoteka, pok. 20

§ 4

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Obszar, o którym mowa w § 2 Polityki bezpieczeństwa, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.

2. Przebywanie osób nieuprawnionych w obszarze, o którym mowa w § 2 Polityki bezpieczeństwa, jest dopuszczalne za zgodą Z ds. ZBI lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

3. Należy zapewnić rejestrację w systemie informatycznym odrębnego identyfikatora i dokonanie uwierzytelnienia.

4. Dostęp do danych może być możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

5. Systemy informatyczne służące do przetwarzania danych osobowych oraz systemy operacyjne należy zabezpieczyć przed:
   – działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
   – utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

6. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.

7. W przypadku gdy do uwierzytelnienia użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło powinno składać się co najmniej z 8 znaków.

8. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przed wykonywaniem kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.

9. Kopie zapasowe:
- przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;
- usuwa się niezwłocznie po ustaniu ich użyteczności.

10. Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza siedzibą Starostwa Powiatowego, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.

11. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

- likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
- przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
- naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

12. Hasła stosowane do uwierzytelniania w systemach informatycznych muszą składać się co najmniej z 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

13. Systemy informatyczne służące do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.

§ 5

Plan awaryjny

1. Plan awaryjny pozwala na odtworzenie bazy komputerowej urzędu i struktury sieci informatycznej w przypadku, gdy w wyniku nieszczęśliwego wypadku zostanie zniszczona lub poważnie uszkodzona.

2. Intencją planu jest przywrócenie systemu do stanu pierwotnego tak szybko jak to możliwe przy pomocy najświeższych i najbardziej aktualnych danych uzyskanych z kopii zapasowej systemu. Wysiłek przy przywracaniu systemu koncentruje się na przywróceniu danych do stanu sprzed wypadku, a także na połączeniu tych danych z nowymi danymi, które zostały zarejestrowane po wypadku, ale jeszcze przed przywróceniem systemu do działania.

3. Zapewnienie awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania. Komputery oraz urządzenia, o których mowa wyżej powinny być zasilane poprzez zastosowanie specjalnych urządzeń podtrzymujących zasilanie. Urządzenia te powinny być wyposażone w oprogramowania umożliwiające bezpieczne wyłączenie systemu komputerowego. Oznacza to takie wyłączenie, w którym przed zanikiem zasilania zostaną prawidłowo zakończone rozpoczęte transakcje na bazie danych oraz wszelkie inne działanie w ramach pracujących aplikacji i oprogramowania systemowego.