Zarządzenie nr 47/07
Wójta Gminy Podgórzyn
z dnia 07 maja 2007r.

w sprawie wprowadzenia „Polityki Bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Podgórzynie".

Na podstawie art. 33 ust. 1 ustawy z dnia 08 marca 1990r. (tekst jednolity Dz.U. z 2001 roku nr 142 poz. 1591 ze zmianami) oraz § 3 ust. 3 i § 4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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.Nr 100, poz. 1024) zarządza się, co następuje:

§ 1

Wprowadza się „Politykę bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Podgórzynie", zwaną dalej polityką bezpieczeństwa.
Treść polityki bezpieczeństwa zawierają załączniki nr: 1, 2, 3, 4 do niniejszego zarządzenia.

§ 2

Polityka bezpieczeństwa ma zastosowanie na wszystkich stanowiskach pracy, gdzie przetwarzane są dane osobowe.

§ 3

Wykonanie zarządzenia powierza się:
1) Administratorowi Bezpieczeństwa Informacji – w zakresie przygotowania infrastruktury technicznej spełniającej wymogi polityki bezpieczeństwa,
2) Kierownikom Referatów Urzędu Gminy – w zakresie wdrożenia oraz przestrzegania polityki bezpieczeństwa.

§ 4

Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJT GMINY
Anna Latto

RADCA PRAWNY
mgr [illegible] Orłowska

Załącznik nr 1

do zarządzenia nr 47/07

Wójta Gminy Podgórzyn

z dnia 07 maja 2007r.

Polityka bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Podgórzyn

Spis treści:

Rozdział 1

Postanowienia ogólne

§ 1

1. „Polityka bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Podgórzyn", zwana dalej Polityką bezpieczeństwa, opracowana została zgodnie z wymogami określonymi w § 4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. nr 100, poz. 1024).

2. Niniejsza Polityka bezpieczeństwa, jest wewnętrznym dokumentem wydanym przez Wójta Gminy Podgórzyn i przeznaczona jest dla osób zatrudnionych przy przetwarzaniu danych osobowych.

§ 2

Określenia i skróty użyte w Polityce bezpieczeństwa oznaczają:

1. Administrator Danych Osobowych – Wójt Gminy Podgórzyn, zwany dalej Administratorem.

2. Administrator Bezpieczeństwa Informacji, zwany dalej ABI – osoba z certyfikatem Bezpieczeństwa Publicznego stanowiący odrębny załącznik wyznaczona przez Administratora lub osobę upoważnioną, odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych Urzędu Gminy Podgórzyn, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemów oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w tych systemach oraz odpowiedzialna za sprawność, konserwacje i wdrażanie technicznych zabezpieczeń systemów informatycznych, w których przetwarzane są dane osobowe w zbiorach komórek organizacyjnych Urzędu Gminy Podgórzyn.

3. Osoba upoważniona lub użytkownik systemu, zwany dalej użytkownikiem – osoba posiadająca upoważnienie wydane przez Administratora lub osobę upoważnioną przez niego i dopuszczona w zakresie w nim wskazanym, jako użytkownik do przetwarzania danych osobowych w systemie informatycznym komórki organizacyjnej Urzędu Gminy Podgórzyn.

5. Przełożony użytkownika, zwany dalej przełożonym – kierownik Referatu Urzędu Gminy Podgórzyn.

6. System informatyczny, zwany dalej systemem, to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

7. Zabezpieczenie systemu informatycznego – wdrożenie przez Administratora stosownych środków organizacyjnych i technicznych w celu zabezpieczenia zasobów oraz ochrony danych przed dostępem, modyfikacją ujawnieniem, pozyskaniem lub zniszczeniem przez osobę trzecią.

8. Przetwarzanie danych osobowych – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, udostępnianie i usuwanie, a zwłaszcza tych, które są wykonywane w systemach informatycznych.

Rozdział 2

Obszar przetwarzania danych osobowych

§ 3

1. Obszar przetwarzania danych osobowych w Urzędzie Gminy Podgórzyn stanowią wszystkie biura urzędu

Rozdział 3

Wykaz zbiorów danych osobowych

§ 4

1. Referat Społeczno-Organizacyjny (sprawy obywatelskie , zarządzania kryzysowe i Urząd Stanu Cywilnego
   W Referacie Społeczno-Organizacyjnym przetwarzane są dane osobowe zgodnie z ustawą o Ewidencji Ludności (Dz. U z 2001, nr 87, poz. 960), w postaci papierowej – Karta Osobowa Mieszkańca oraz w postaci elektronicznej – program ARAM - Ewidencja Ludności oraz ARAM – Dowody Osobiste.

2. Kadry i Płace
   W biurach tych przetwarzane są dane osobowe pracowników Urzędu Gminy Podgórzyn, zgodnie z ustawą z dnia 26 czerwca 1974 r. – kodeks pracy (Dz. U. nr 24, poz. 141 z późn. zm.), w postaci papierowej – akta pracownika oraz w postaci elektronicznej – program SIGID i PŁATNIK (pracujący pod kontrolą systemu sieciowego NetWare 4.12)

3. Referat Finansowy
   W Referacie Finansowym przetwarzane są dane osobowe płatników opłat i podatków, zgodnie z Rozporządzeniem Ministra Finansów z dnia 22 kwietnia 2004 r. w sprawie ewidencji podatkowej nieruchomości (Dz. U. z 2004 r. Nr 107, poz. 1138) oraz zgodnie z ustawą z dnia 26 czerwca 1974 r. – kodeks pracy (Dz. U. nr 24, poz. 141 z późn. zm.) w postaci papierowej – wydruki komputerowe oraz elektronicznie. Do przetwarzania danych osobowych służy oprogramowanie: SIGID, Program BANKOWY, (pracujący pod kontrolą systemu sieciowego NetWare 4.12)

4. Referat Rozwoju
   W Referacie Rozwoju przetwarzane są dane osobowe w postaci elektronicznej – program „EGB 2000"

Rozdział 4

Opis struktury zbiorów

§ 5

Struktura zbiorów danych osobowych

1. System ARAM zasilają system Ewidencja Ludności. – pliki bazodanowe - Irfomix + SQL
2. System „SIGID" – pliki bazodanowe - DBF
3. System „EGB 2000" – pliki bazodanowe SQL

Rozdział 5

Sposób przepływu danych pomiędzy poszczególnymi systemami służącymi do przetwarzania danych osobowych

§ 6

4. Informacje z systemu ARAM zasilają system Ewidencja Ludności. Dane są wprowadzane z wydruków komputerowych.

5. Informacje z systemu „SIGID" zasilają system „SIGID". Dane są wprowadzane z wydruków komputerowych oraz automatycznie.

6. Informacje z systemu „EGB 2000" zasilają system „EGB 2000". Dane są wprowadzane z wydruków komputerowych oraz automatycznie.

7. Informacje z systemu „SIGID" zasilają systemy „Płatnik", „BANK". Dane są wprowadzane z wydruków komputerowych jak i w wersji elektronicznej

Załącznik nr 2
do zarządzenia nr 47/07
Wójta Gminy Podgórzyn
z dnia 07 maja 2007r.

Instrukcja zarządzania systemem informatycznym oraz środki techniczne i organizacyjne niezbędne do zapewnienia poufności i rozliczania danych

A. Środki ochrony fizycznej

1. Budynek Urzędu, w którym zlokalizowany jest obszar przetwarzania danych osobowych jest nadzorowany przez firmę ochroniarską
2. Pomieszczenia urzędu posiadają alarm.
3. Urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych zamkami patentowymi.
4. Przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osoby zatrudnionej przy przetwarzaniu danych lub w obecności Administratora Bezpieczeństwa Informacji.
5. Pomieszczenia, o których mowa wyżej, powinny być zamykane na czas nieobecności pracownika zatrudnionego przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.
6. W przypadku przebywania interesantów bądź innych osób postronnych w 2 pomieszczeniach, o których mowa wyżej, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.
7. Do przebywania w pomieszczeniu serwera uprawnieni są: Administrator Bezpieczeństwa Informacji, osoba odpowiedzialna za obsługę informatyczną urzędu oraz Administrator Danych.
8. Przebywanie w pomieszczeniu serwera osób nieuprawnionych (konserwator, elektryk) dopuszczalne jest tylko w obecności jednej z osób upoważnionych, o których mowa w pkt. 7.

B. Środki sprzętowe, informatyczne i telekomunikacyjne

1. Każdy dokument papierowy zawierający dane osobowe przeznaczony do wyrzucenia powinien być zniszczony w sposób uniemożliwiający jego odczytanie , przy pomocy niszczarki, która umożliwia cięcie poprzeczne.
2. Urządzenia wchodzące w skład systemu informatycznego podłączone są do odrębnego obwodu elektrycznego, zabezpieczonego na wypadek zaniku napięcia albo awarii w sieci zasilającej UPS-em.
3. Na stanowiskach pracy, w których przetwarzane są dane osobowe zastosowano oprogramowanie do tworzenia kopii zapasowych.
4. Na serwerze oraz w poszczególnych stacjach roboczych zainstalowano oprogramowanie antywirusowe. Poczta elektroniczna wpływająca do Urzędu skanowana jest programem antywirusowym przed przesłaniem jej do użytkownika.
5. Kopie awaryjne wykonywane są w cyklach:
- tygodniowym na dysku twardym,
- miesięczna na płycie DVD-R.

C. Środki ochrony w ramach oprogramowania systemu

1. Dostęp fizyczny do baz danych osobowych zastrzeżony jest wyłącznie dla osoby zajmującej się obsługą informatyczną urzędu, Administratora Bezpieczeństwa Informacji.
2. Konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych jedynie za pośrednictwem aplikacji.
3. System informatyczny z jakiego korzystają pracownicy urzędu gminy pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu.

D. Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych

1. Zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji.
2. Dla każdego użytkownika systemu jest ustalony odrębny identyfikator.
3. Zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (unikalny identyfikator i hasło).

E. Środki ochrony w ramach systemu użytkowego

1. Zastosowano wygaszanie ekranu w przypadku dłuższej nieaktywności użytkownika.
2. Komputer, z którego możliwy jest dostęp do danych osobowych zabezpieczony jest hasłem uruchomieniowym (BIOS), hasłem wejściowym do systemu operacyjnego oraz hasłem do każdej aplikacji przy pomocy której przetwarzane są dane osobowe.

Załącznik Nr 3
do zarządzenia nr 47/07
Wójta Gminy Podgórzyn
z dnia 07 maja 2007r.

Procedura wykonywania kopii awaryjnych oraz sposobu ich przechowywania

w Urzędzie Gminy w Podgórzynie

Niniejsza procedura określa sposób wykonywania kopii awaryjnych i wydruków danych oraz miejsca ich przechowywania i sposób niszczenia.

§ 1

Nośniki informacji, kartoteki i wydruki komputerowe zawierające dane osobowe przechowuje się wyłącznie wówczas, gdy jest to konieczne i dozwolone przepisami prawa. Przechowuje się je w wyznaczonych pomieszczeniach w których odbywa się przetwarzanie danych, w szafach i innych meblach biurowych wyposażonych w zamki uniemożliwiające dostęp osób niepowołanych.

§ 2

Zgodnie z zasadami zarządzania systemami informatycznymi kopie awaryjne danych z systemów w których przetwarza się dane osobowe wykonywane są :
- kopie bieżące - codziennie regularnie z wykorzystaniem płyt CDR i CD-RW, w systemie umożliwiającym odtworzenie danych z kopii poprzedniej. Kopie wykonywane są po zakończeniu pracy i wylogowaniu się wszystkich użytkowników z sieci informatycznej.

§ 3

Wykonane kopie przechowywane są w szafie opancerzonej zabezpieczone przed dostępem do nich osób niepowołanych w sposób następujący:

- wewnętrzne ściany pokoju gwarantują trwałe oddzielenie ich od innych pomieszczeń,
- pełne drzwi wejściowe antywłamaniowe, zaopatrzone są w co najmniej 1 zamek patentowy,
- okna pokoi są odpowiednio zabezpieczone przed dostępem z zewnątrz
- budynek nadzorowany jest systemem alarmowym
- szafa wykonana jest z metalu zabezpieczona odpowiednim zamkiem,
- klucze do pokoju i szafy posiada upoważniony pracownik wykonujący kopie .

Wydruki zawierające dane osobowe przechowywane są odpowiednio w pokojach w których następuje przetwarzanie danych zabezpieczone przed dostępem osób niepowołanych w sposób następujący:

- wewnętrzne ściany pokoi gwarantują trwałe oddzielenie ich od innych pomieszczeń,
- drzwi wejściowe do pokoi zaopatrzone są w co najmniej 1 zamek patentowy,
- budynek nadzorowany jest systemem alarmowym
- okna pokoi są odpowiednio zabezpieczone przed dostępem z zewnątrz
- szafy i meble biurowe są odpowiednio zabezpieczone zamkami,
- klucze do poszczególnych pokoi, szaf i mebli posiadają upoważnieni pracownicy
- po zakończeniu pracy klucze do pomieszczeń przechowywane są w przeznaczonej do tego szafie w Sekretariacie Urzędu .

Nośniki danych zawierające kopie zdezaktualizowane lub niepoprawnie zapisane niszczone są w sposób mechaniczny.

Wydruki nie wykorzystane, przedawnione, przeznaczone do zniszczenia mielone są natychmiast w niszczarce do papieru.

ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI

A. Szmit

.....