ZARZĄDZENIE NR 302/09
Wójta Gminy Chodzież
z dnia 31 grudnia 2009 r.

w sprawie ustalenia polityki bezpieczeństwa danych osobowych w Urzędzie Gminy w Chodzieży

Na podstawie §3 ust.3 oraz §4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy teleinformatyczne służące do przetwarzania danych osobowych (Dz. U z 2004 r. nr 100, poz. 1024) , zarządza się, co następuje:

§ 1

Ustala się „Politykę Bezpieczeństwa Danych Osobowych w Urzędzie Gminy w Chodzieży" zwaną dalej „Polityką", która stanowi załącznik do niniejszego zarządzenia.

§ 2

Zobowiązuje się pracowników Urzędu Gminy w Chodzieży do stosowania zasad określonych w „Polityce"

§ 3

Wykonanie zarządzenia powierza się Administratorowi Danych Osobowych.

§ 4

Zarządzenie obowiązuje od dnia podpisania.

WÓJT
mgr Zbigniew Salwa

UZASADNIENIE

do Zarządzenia Nr 302/09 r. Wójta Gminy Chodzież z dnia 31 grudnia 2009 r.

Na podstawie §3 ust.3 oraz §4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy teleinformatyczne służące do przetwarzania danych osobowych (Dz. U z 2004 r. nr 100, poz. 1024). W celu określenia zasad bezpieczeństwa danych osobowych Administrator Danych Osobowych ustala odpowiednią dokumentację, w tym politykę bezpieczeństwa.

WÓJT

mgr Zbigniew Salwa

Załącznik Nr 1
do Zarządzenia nr 302/09
Wójta Gminy Chodzież
z dnia 31 grudnia 2009 r.

Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Chodzież

I. Wprowadzenie

Celem Instrukcji Zarządzania System Informatycznym jest zapewnienie bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy w Chodzieży, oraz minimalizowanie incydentów mogących zagrozić bezpieczeństwu systemu.
Podstawa prawna tego dokumentu:

- rozporządzenie Ministra Spraw Wewnętrznych i Administracji 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. Nr 100, poz. 1024)
- ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Z 2002 r. Nr 101, poz. 926 z późn. zm.)

II. Definicje

Ilekroć w niniejszym dokumencie jest mowa o:

a. urzędzie – należy przez to rozumieć Urząd Gminy w Chodzieży,
b. Administratorze Danych Osobowych – należy przez to rozumieć Wójta Gminy Chodzież,
c. Administratorze Bezpieczeństwa Informacji – należy przez to rozumieć pracownika urzędu lub inną osobę wyznaczoną do nadzorowania przestrzegania zasad ochrony, określonych w niniejszym dokumencie, Polityce Bezpieczeństwa Danych Osobowych w Urzędzie Gminy Chodzież, oraz wymagań w zakresie ochrony wynikających z powszechnie wynikających przepisów o ochronie danych osobowych,
d. Administratorze Systemu Informatycznego – informatyk odpowiedzialny za funkcjonowanie systemu, oraz stosowanie technicznych i organizacyjnych środków ochrony stosowanych w tym systemie,
e. użytkownika systemu - osoba upoważniona do przetwarzania danych osobowych w systemie. Użytkownikiem może być osoba zatrudniona w urzędzie, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w urzędzie,
f. sieci lokalnej - połączenie komputerów pracujących w urzędzie w celu wymiany danych (informacji) dla własnych potrzeb, przy wykorzystaniu urządzeń telekomunikacyjnych,
g. sieci rozległej (publicznej) - sieć telekomunikacyjna, nie będąca siecią wewnętrzną służąca do świadczenia usług telekomunikacyjnych w rozumieniu ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z pożń. zm.),
h. danych osobowych - rozumie się przez to wszystkie informacje dotyczące zidentyfikowanej lub możliwej od zidentyfikowania osoby fizycznej,

i. zbiorze danych – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych wg określonych kryteriów,
j. wykazie zbiorów danych osobowych – rozumie się przez to wykaz zarejestrowanych jak i nie podlegających rejestracji zbiorów danych osobowych,
k. przetwarzaniu danych - rozumie się to w tym dokumencie jako jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemie informatycznym,
l. systemie informatycznym - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

III. *Procedury nadawania i zmiany uprawnień do przetwarzania danych osobowych w systemie informatycznym*

1. Każdy użytkownik systemu informatycznego przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:
   a. polityką bezpieczeństwa danych osobowych w Urzędzie Gminy Chodzież
   b. niniejszym dokumentem
2. Zapoznanie się z powyższymi informacjami pracownik potwierdza własnoręcznym podpisem na wykazie, którego wzór stanowi Załącznik nr 4 do „Polityki bezpieczeństwa danych osobowych w Urzędzie Gminy Chodzież"
3. Przetwarzanie danych osobowych może dokonywać jedynie pracownik posiadający upoważnienie przez Administratora Danych Osobowych (załącznik nr 5 do „Polityki bezpieczeństwa danych osobowych w Urzędzie Gminy Chodzież").
4. Administrator Bezpieczeństwa Informacji przyznaje uprawnienia w zakresie dostępu do systemu informatycznego służącego do przetwarzania danych osobowych na podstawie pisemnego upoważnienia Administratora Danych Osobowych określającego zakres uprawnień pracownika, którego wzór stanowi załącznik nr 5 do „Polityki bezpieczeństwa danych osobowych w Urzędzie Gminy Chodzież".
5. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora, hasła, oraz ustanowienia zakresu dostępnych danych i operacji.
6. Hasło ustanowione podczas przyznawania uprawnień przez Administratora Bezpieczeństwa Informacji jest przekazywane użytkownikowi ustnie. Hasło to należy zmienić na indywidualne podczas pierwszego logowania się w systemie informatycznym.
7. Pracownik ma prawo do wykonywania tylko tych czynności do jakich został upoważniony.
8. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła.
9. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako naruszenie podstawowych obowiązków pracowniczych.
10. Pracownik zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest do zachowania ich w tajemnicy. Tajemnica obowiązuje go również po ustaniu zatrudnienia
11. W systemie informatycznym stosuje się uwierzytelnienie dwustopniowe: na poziomie dostępu do sieci lokalnej, oraz dostępu do aplikacji.
12. Odebranie uprawnień pracownikowi następuje na wniosek Administratora Danych Osobowych z podaniem daty i przyczyny odebrania uprawnień

13. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane, oraz unieważnić jej hasło.
14. Administrator Bezpieczeństwa Informacji zobowiązany jest do prowadzenia, ochrony rejestru użytkowników, oraz ich uprawnień w systemie informatycznym.
15. Rejestr powinien odzwierciedlać aktualny stan systemu w zakresie użytkowników i ich uprawnień, oraz umożliwiać przeglądanie historii zmian uprawnień użytkowników.

IV. Zasady ustalania i posługiwania się hasłami.

1. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
2. Hasło użytkownika musi być zmienione przynajmniej raz w miesiącu.
3. Identyfikator użytkownika nie powinien być zmieniany bez wyraźniej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.
4. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł.
5. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
6. Pracownik nie ma prawa udostępniania swojego hasła innym osobom.
7. Hasło należy wprowadzać w sposób który uniemożliwi innym osobom jego poznanie.
8. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła.
9. Przy wyborze hasła występują następujące zasady
   a. minimalna długość hasła to 6 znaków,
   b. zakazuje się stosować
      - haseł, z których użytkownik korzystał w poprzednim miesiącu,
      - swojej nazwy użytkownika w jakiejkolwiek formie,
      - swojego nazwiska czy imienia w jakiejkolwiek formie
      - ogólnie dostępnych informacji o użytkowniku takich jak numer telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego, nazwa ulicy na której mieszka itp.
      - przewidywalnych sekwencji znaków z klawiatury np. „QWERTY”,”12345” itp.
   c. należy stosować:
      - hasła zawierające kombinacje liter i cyfr,
      - hasła które można zapamiętać bez zapisywania.
10. Zmiany hasła nie można zlecać innym osobom.

V. Procedury rozpoczęcia, zawieszania i zakończenia pracy w systemie.

1. Przed rozpoczęciem pracy z komputerem należy zalogować się do systemu informatycznego przy użyciu własnego indywidualnego identyfikatora i hasła.
2. W sytuacji opuszczenia stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wylogować się z systemu.
3. Przed wyłączeniem komputera należy zakończyć pracę wszystkich używanych programów i wykonać o ile to możliwe prawidłowe zamknięcie systemu.
4. Niedopuszczalne jest wyłączanie komputera bez prawidłowego zamknięcia wszystkich programów i wylogowania z sieci komputerowej.

5. Przypadki nieprawidłowej pracy systemu informatycznego należy niezwłocznie zgłaszać do administratora systemu informatycznego.

VI. Kopie bezpieczeństwa danych osobowych.

1. Kopie bezpieczeństwa danych osobowych przygotowywane są przez Administratora Systemu Teleinformatycznego.
2. Kopie wykonywane są raz na tydzień na płytach DVD
3. Płyty DVD po archiwizacji przechowywane są w szafie stalowej w zamkniętym pomieszczeniu.
4. Co kwartał następuje klasyfikacja nośników DVD do dalszej przydatności.
5. Niepotrzebne płyty DVD niszczone są w specjalnej niszczarce do nośników optycznych.

VII. Przechowywanie elektronicznych nośników informacji zawierających dane osobowe oraz wydruków.

1. Elektroniczne nośniki informacji
   a. Dane osobowe w postaci elektronicznej (nie licząc kopii bezpieczeństwa) zapisane na dyskietkach, dyskach magnetooptycznych, dyskach twardych nie można wynosić poza siedzibę urzędu.
   b. Wymienne elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych (określony w Polityce Bezpieczeństwa Danych Osobowych Urzędu Gminy w Chodzieży).
   c. Po zakończeniu pracy przez użytkowników systemu, elektroniczne nośniki informacji są przechowywane wyłącznie w zamykanych szafach biurowych.
   d. Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymywania danych osobowych pozbawia się wcześniej zapisu tych danych.
   e. Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych. W przypadku gdy nie jest to możliwe uszkadza się je w sposób uniemożliwiający ich odczytanie.
   f. Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej.
2. Wydruki
   a. W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym dostęp osobom nieuprawnionym.
   b. Pomieszczenie w którym przechowywane są wydruki musi być zamknięte na klucz po godzinach pracy urzędu.
   c. Wydruki zawierające dane osobowe w momencie przekazania do usunięcia są niszczone w sposób uniemożliwiający ich odczytanie (w specjalnej niszczarce do papieru).

VIII. Ochrona przed złośliwym oprogramowaniem.

1. Każdy komputer służący do przetwarzania danych osobowych jest wyposażony w działający cały czas program antywirusowy z wbudowanym zaporą sieciową (firewall). Program antywirusowy aktualizowany jest automatycznie przynajmniej raz na dwie godziny.

2. Cały ruch sieciowy z siecią publiczną monitorowany jest na bieżąco przez bramę antywirusową w routerze sieciowym.
3. Zabrania się stosowania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Za skanowanie odpowiedzialny jest użytkownik komputera.
4. Poczta elektroniczna jest automatycznie sprawdzana przez skaner antywirusowy.
5. Wykrycie wirusa użytkownik komputera ma obowiązek zgłosić natychmiast administratorowi systemu informatycznego.

IX. Połączenie do sieci Internet.

1. Połączenie z siecią Internet (siecią publiczną) zabezpieczone jest przez moduł firewall działający na routerze sieciowym.
2. Na każdym komputerze w systemie informatycznym urzędu działa osobny firewall.
3. Zabronione jest połączenie z siecią Internet z niedziałającym programem antywirusowym (lub jego brakiem) i firewallem.

WÓJT
mgr Zbigniew Salwa