WÓJT GMINY
PRUSZCZ GDAŃSKI
ul. Wojska Polskiego 30
83-000 Pruszcz Gdański

Zarządzenie Nr 71/2004
Wójta Gminy Pruszcz Gdański
z dnia 27 grudnia 2004r.

w sprawie wdrożenia Instrukcji zarządzania systemem informatycznym Urzędu Gminy Pruszcz Gdański

Na podstawie § 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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. 1. Z dniem 1 stycznia 2005r. wdraża się Instrukcję zarządzania systemem informatycznym Urzędu Gminy Pruszcz Gdański.

2. Instrukcja o której mowa w ust. 1 stanowi załącznik do niniejszego zarządzenia.

§ 2. Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJT
Magdalena Kołodziejczak

Załącznik nr 1
do Zarządzenia nr 71/2004
z dnia 27 grudnia 2004

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM URZĘDU GMINY PRUSZCZ GDAŃSKI

Podstawa prawna:

- 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.)

I. Definicje.

Ilekroć w niniejszym dokumencie jest mowa o:

a) Urzędzie – należy przez to rozumieć Urząd Gminy Pruszcz Gdański,

b) Administratorze Danych – należy przez to rozumieć Wójta Gminy Pruszcz Gdański,

c) Administratorze Bezpieczeństwa Informacji – należy przez to rozumieć pracownika Urzędu lub inną osobę wyznaczoną do nadzorowania przestrzegania zasad ochrony danych osobowych ustanowionego zgodnie z Polityką bezpieczeństwa przetwarzania danych osobowych Urzędu,

d) Administratorze Systemu Informatycznego – należy przez to rozumieć osobę odpowiedzialną za funkcjonowanie systemu informatycznego Urzędu oraz stosowanie technicznych i organizacyjnych środków ochrony,

e) użytkowniku systemu – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym Urzędu. Użytkownikiem może być pracownik Urzędu, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w Urzędzie lub wolontariusz,

f) sieci lokalnej – należy przez to rozumieć połączenie systemów informatycznych Urzędu wyłącznie dla własnych jej potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych,

g) sieci rozległej – należy przez to rozumieć sieć publiczną w rozumieniu ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.)

II Procedury nadawania i zmiany uprawnień do przetwarzania danych.

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:

- Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 Nr 101, poz. 926 z późn. zm.),
- Polityką bezpieczeństwa przetwarzania danych osobowych systemu informatycznego, - niniejszym dokumentem.

2. Administrator Bezpieczeństwa Informacji przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnego upoważnienia (wniosku) administratora danych określającego zakres uprawnień pracownika, którego wzór stanowi Załącznik Nr 1 do niniejszego opracowania.
3. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora, hasła oraz zakresu dostępnych danych i operacji.
4. Hasło ustanowione podczas przyznawania uprawnień przez Administratora Bezpieczeństwa Informacji należy zmienić na indywidualne podczas pierwszego logowania się w systemie informatycznym. Ustanowione hasło, administrator przekazuje użytkownikowi ustnie.
5. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.
6. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
7. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako naruszenie podstawowych obowiązków pracowniczych.
8. Pracownik zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest do zachowania ich w tajemnicy. Tajemnica obowiązuje go również po ustaniu zatrudnienia.
9. W systemie informatycznym stosuje się uwierzytelnianie trzystopniowe: na poziomie dostępu do systemu, serwera plików oraz dostępu do aplikacji.
10. Identyfikator użytkownika w aplikacji (o ile działanie aplikacji na to pozwala), powinien być tożsamy z tym, jaki jest mu przydzielany do serwera plików.
11. Odebranie uprawnień pracownikowi następuje na pisemny wniosek kierownika, któremu pracownik podlega z podaniem daty oraz przyczyny odebrania uprawnień.
12. Kierownicy komórek organizacyjnych zobowiązani są pisemnie informować Administratora Bezpieczeństwa Informacji o każdej zmianie dotyczącej podległych pracowników mającej wpływ na zakres posiadanych uprawnień w systemie informatycznym.
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 i ochrony rejestru użytkowników i ich uprawnień w systemie informatycznym.
15. Rejestr, którego wzór stanowi Załącznik Nr 2, powinien zawierać:

- imię i nazwisko użytkownika systemów informatycznych,
- rodzaj uprawnienia,

- datę nada uprawnienia,
- przyczynę odebrania uprawnienia,
- podpis administratora bezpieczeństwa informacji.

16. Rejestr powinien odzwierciedlać aktualny stan systemu w zakresie użytkowników i ich uprawnień oraz umożliwiać przeglądanie historii zmian uprawnień użytkowników.

III. Zasady posługiwania się hasłami.

. Każdy komputer PC przetwarzający dane osobowe jest zabezpieczony przed uruchomieniem przez niepowołaną osobę przy pomocy hasła do systemu operacyjnego:

Obowiązują następujące zasady korzystania z tego hasła:

•hasło jest obowiązkowe dla każdego komputera PC przetwarzającego dane osobowe
•hasło jest zakładane przez administratora, który następnie podaje je do wiadomości użytkownika komputera
•hasło jest ciągiem co najmniej 8 znaków, musi zawierać zarówno litery jak i cyfry lub inne znaki,
•przy wpisywaniu hasła nie jest ono wyświetlane na ekranie,
•hasło musi być zmieniane przynajmniej raz na 30 dni
•w przypadku ujawnienia hasła osobom nieupoważnionym musi ono zostać niezwłocznie zmienione,
•za systematyczną zmianę haseł odpowiada użytkownik

Programy przy pomocy których przetwarzane są dane osobowe – użyto zaimplementowanych narzędzi baz danych do ograniczenia dostępu do zbiorów za pomocą unikalnego logiku i hasła.

Dodatkowo dostęp do serwera plików zabezpieczony jest również loginem i hasłem

IV. Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie.

1. Przed rozpoczęciem pracy w systemie komputerowym należy zameldować się do systemu oraz serwera plików przy użyciu indywidualnego identyfikatora oraz hasła.
2. Przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wykonać opcję wymeldowania z systemu (zablokowania dostępu), lub jeżeli taka możliwość nie istnieje wyjść z programu.
3. Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązana jest wykonać funkcję wymeldowania z systemu.
4. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów, wykonać zamknięcie systemu i jeżeli jest to konieczne wymeldować się z sieci komputerowej.
5. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania oraz zakończeniem pracy w sieci.

V. Procedury tworzenia zabezpieczeń.

1. Za systematyczne przygotowanie kopii bezpieczeństwa odpowiada Administrator Bezpieczeństwa Informacji, a w przypadku jego nieobecności Administrator Systemu Informatycznego.
2. Kopie zapasowe danych na serwerze sporządzane są codziennie, na stanowiskach roboczych raz w tygodniu. Tak sporządzone kopie zapisywane są na trwały nośnik (CD-R/DVD-R) co najmniej raz w tygodniu.
3. Płyty CD-R/DVD-R przechowuje się w kasie pancernej w budynku Urzędu Gminy w Pruszczu Gdańskim ul. Wojska Polskiego 30.
4. Kopie danych powinny być okresowo sprawdzane pod kątem ich przydatności – prawidłowości wykonania oraz możliwości odtworzenia.
5. Kopia systemu operacyjnego powinna być wykonywana po każdej modyfikacji, zmianie konfiguracji i instalacji nowej wersji nie rzadziej niż raz w miesiącu.

VI. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe.

A. Elektroniczne nośniki informacji.

1. Dane osobowe w postaci elektronicznej - za wyjątkiem kopii bezpieczeństwa – zapisane na dyskietkach, dyskach magnetooptycznych czy dyskach twardych nie są wynoszone poza siedzibę Urzędu.
2. Wymienne elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych, określony w Polityce bezpieczeństwa przetwarzania danych osobowych Urzędu.
3. Po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki informacji są przechowywane w zamykanych szafach biurowych lub kasetkach.
4. Urządzenia, dyski lub inne informatyczne nośniki, 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.
5. 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.
6. 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.

B. Kopie zapasowe.

1. Kopie zapasowe zbioru danych osobowych oraz oprogramowania i narzędzi

programowych zastosowanych do przetwarzania danych przechowywane są w sejfie w budynku Urzędu Gminy w Pruszczu Gdańskim ul. Wojska Polskiego 30.

2. Dostęp do danych opisanych w punkcie 1 ma Administrator Bezpieczeństwa Informacji oraz upoważnieni przez Administratora Danych pracownicy.

VII. Środki ochrony systemu przed złośliwym oprogramowaniem, w tym wirusami komputerowymi.

1. Na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe pracujące w trybie monitora.
2. Każdy e-mail wpływający do Urzędu musi być sprawdzony pod kątem występowania wirusów przez bramę antywirusową.
3. Definicje wzorców wirusów aktualizowane są nie rzadziej niż raz dziennie.
4. Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje użytkownik, który nośnik zamierza użyć.
5. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.
6. Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje pracownik, który pocztę otrzymał.
7. Administrator Systemu Informatycznego przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach - minimum raz na miesiąc.
8. Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania.
9. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe na którym wirusa wykryto oraz wszystkie posiadane przez użytkownika nośniki danych.

VIII. Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych.

1. Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie osobom upoważnionym.
2. Udostępnienie danych osobowych, w jakiejkolwiek postaci, jednostkom nieuprawnionym wymaga pisemnego upoważnienia Administratora Danych.
3. Kierownicy komórek organizacyjnych prowadzą rejestry udostępnionych danych osobowych zawierające co najmniej: datę udostępnienia, podstawę, zakres udostępnionych informacji oraz osobę lub instytucję dla której dane udostępniono.

IX. Sposób postępowania w sytuacji naruszenia ochrony danych osobowych.

Sposób postępowania w sytuacji stwierdzenia naruszenia ochrony danych osobowych określa instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych (Zarządzenie nr 7/99 Wójta Gminy Pruszcz Gdański z 15 sierpnia 1999 roku)

X. Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych.

1. Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie osobom upoważnionym.
2. Udostępnienie danych osobowych, w jakiejkolwiek postaci, jednostkom nieuprawnionym wymaga pisemnego upoważnienia Administratora Danych.
3. Udostępnienie danych osobowych nie może być realizowane drogą telefoniczną.

XI. Procedury wykonywania przeglądów i konserwacji systemu.

1. Przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być dokonywane w terminach określonych przez producenta sprzętu, nie rzadziej niż raz do roku.
2. Przegląd oprogramowania i baz danych przeprowadzana jest zgodnie z zaleceniami twórców poszczególnych programów nie rzadziej niż raz na miesiąc i obejmuje:

   - instalacja łatek, poprawek i zestawów poprawek

   - sprawdzenie systemu komputerowego pod katem obecności oprogramowania szpiegowskiego

   - przegląd dzienników zdarzeń systemów, w szczególności dziennika systemu i dziennika aplikacji pod kątem ewentualnych błędów

3. Nieprawidłowości ujawnione w trakcie tych działań powinny być usunięte, a ich przyczyny przeanalizowane.

WÓJT

Magdalena Kołodziejczak

ZAŁĄCZNIK NR 1
DO INSTRUKCJI ZARZĄDZANIA
SYSTEMEM INFORMATYCZNYM

WNIOSEK
O NADANIE UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

☐ **Nowy użytkownik**	☐ **Modyfikacja uprawnień**	☐ **Odebranie uprawnień w systemie informatycznym**

Imię i nazwisko użytkownika:	**Zespół/ Wydział**
Opis zakresu uprawnień użytkownika w systemie informatycznym i uzasadnienie:	
Data wystawienia:	Podpis bezpośredniego przełożonego użytkownika systemu:
	Podpis Kierownika Urzędu

ZAŁĄCZNIK NR 2
DO INSTRUKCJI ZARZĄDZANIA
SYSTEMEM INFORMATYCZNYM

REJESTR UŻYTKOWNIKÓW I UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

KARTA EWIDENCYJNA UPRAWNIEŃ OSOBY UPOWAŻNIONEJ DO PRZETWARZANIA DANYCH OSOBOWYCH

Identyfikator użytkownika	*Nazwisko i imię*

Lp.	Zakres upoważnienia	Data nadania uprawnień	Podpis osoby upoważnionej	Data i przyczyna odebrania uprawnień
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				