Załącznik nr 3
do zarządzenia nr 117/2008

Instrukcja postępowania
w sytuacji naruszenia systemu ochrony danych osobowych

§ 1

Instrukcja jest przeznaczona dla osób zatrudnionych przy przetwarzaniu danych osobowych.

§ 2

Instrukcja określa tryb postępowania w przypadku gdy:
1. stwierdzono naruszenie zabezpieczenia systemu informatycznego lub naruszenie zabezpieczenia zbioru danych osobowych zebranych i przetwarzanych w innej formie,
2. stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej,

mogą wskazywać na naruszenie zabezpieczeń tych danych.

§ 3

1. Każda osoba zatrudniona w Urzędzie Gminy w Osięcinach, która stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych w systemie informatycznym (lub przetwarzanych w inny sposób), powinna niezwłocznie poinformować o tym osobę zatrudnioną przy przetwarzaniu danych osobowych lub administratora bezpieczeństwa informacji, albo inna upoważnioną przez niego osobę.
2. Osoba zatrudniona przy przetwarzaniu danych osobowych, która uzyskała informację lub sama stwierdziła naruszenie zabezpieczenia bazy danych osobowych, zobowiązana jest niezwłocznie powiadomić o tym administratora bezpieczeństwa informacji.

§ 4

1. Dane osobowe zostają ujawnione, gdy stają się znane w całości lub części pozwalającej na określenie osobom nie uprawnionym tożsamości osoby, której dane dotyczą.
2. W stosunku do danych, które zostały zagubione, pozostawione bez nadzoru poza obszarem bezpieczeństwa należy przeprowadzić postępowanie wyjaśniające, czy dane osobowe należy uznać za ujawnione.

§ 5

Niezwłocznie po uzyskaniu informacji o naruszeniu danych osobowych należy podjąć działania w celu powstrzymania lub ograniczenia dostępu do danych przez osoby niepowołane, poprzez:
1. fizyczne odłączenie urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nie uprawnionej,
2. wylogować użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych,
3. zmianę hasła na konto administratora bezpieczeństwa informacji i użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania,
4. zamknięcie i opieczętowanie urządzeń, w których przechowywane są dane osobowe w formie analogowej.

§ 6

Administrator bezpieczeństwa informacji, po uzyskaniu sygnału o naruszeniu danych osobowych, powinien w pierwszej kolejności:
1. zapisać wszelkie informacje związane z danym zdarzeniem,
2. na bieżąco wygenerować i wydrukować wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia,
3. przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby niepowołanej,
4. wyniki postępowania zabezpieczającego oraz okoliczności naruszenia bezpieczeństwa danych osobowych należy ująć w raporcie i niezwłocznie przekazać Wójtowi Gminy Osięciny.

§ 7

1 Po dokonaniu czynności zabezpieczenia danych osobowych i ustaleniu przyczyn naruszenia ochrony danych osobowych należy niezwłocznie przywrócić normalny stan działania
2 Po przywróceniu prawidłowego stanu bazy danych osobowych, należy przeprowadzić szczegółową analizę, w celu określenia przyczyna naruszenia ochrony danych osobowych oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
3 Jeżeli przyczyną zdarzenia był błąd osoby zatrudnionej przy przetwarzaniu danych osobowych, należy przeprowadzić dodatkowe szkolenie osób biorących udział przy przetwarzaniu danych osobowych.

§ 8

W zakresie nieuregulowanym niniejszą instrukcją, stosuje się odpowiednie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. NR 80, poz. 521).

Wójt Gminy
mgr Jerzy Izydorski

Załącznik nr 4
do zarządzenia nr 117/2008

.....
nazwa urzędu

Wykaz baz danych w systemach informatycznych w których przetwarzane są dane osobowe

Lp	Nazwa bazy danych[1]	Wersja bazy danych	Forma bazy danych/System operacyjny serwera[2]	Sposób zabezpieczenia informatycznego[3]	Zawiera także dane osób spoza firmy (T/N)	Baza danych chroniona przez UPS (T/N)	Liczba miejsc przetwarzania i liczba porządkowa w załączniku nr 3

[1]nazwa zwyczajowa lub własna, np. kadry, itp.
[2]np. plik Excela/Windows 2000
[3]np. (I) indywidualne hasło dostępu do bazy danych, (S) szyfrowanie bazy danych, (F) wydzielona fizycznie sieć
[4]np. kontrola dostępu

Załącznik nr 5
do zarządzenia nr 117/2008

.....
nazwa urzędu

Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych i ich identyfikatorów

Lp	Nazwa bazy danych [1]	Nazwisko i imię użytkownika	Nazwa identyfika-tora	Rodzaj uprawnień[2]	Data zarejest.	Data wyrejest.	Lokalizacja [3]	Uwagi

[1]Nazwa bazy danych z załącznika nr 1
[2]Skróty stosowane do określenia uprawnień
Z – pełne prawa do zarządzania bazą danych
W – pełne prawa do edycji danych (w tym drukowania, archiwizowania, usuwania)
N – prawo do zakładania nowych kont
M – prawo do dodawania i modyfikacji danych
P – prawo do przeglądania danych na ekranie
D – prawo do drukowania danych
A – prawo do wykonywania kopii archiwalnych
Uwaga: w przypadku praw ograniczonych do określonej części bazy danych (np. studentów określonego kierunku studiów) należy ograniczenie to podać w polu Uwagi
[3]należy podać liczbę porządkową zgodnie z załącznikiem nr 3

Dane aktualne na dzień:...../...../.....

Sporządził:.....

Załącznik nr 6
do zarządzenia nr 117/2006

.....
nazwa urzędu

Wykaz miejsc przetwarzania danych osobowych w systemach informatycznych

UWAGA: do każdej lokalizacji należy dołączyć szkic sytuacyjny określający położenie stanowisk komputerowych w pomieszczeniu, z zaznaczeniem strefy ochronnej do której nie mają dostępu osoby nieupoważnione, drzwi wejściowe, okna oraz zabezpieczenia fizyczne.

Lp.	Nazwa bazy danych[1]	Lokalizacja (adres)	Nr pokoju /piętro	Funkcja lokalizacji [2]	Zabezpieczenie fizyczne [3]

[1]nazwa bazy danych z załącznika nr 1
[2](S) - serwer, (K) – miejsce przechowywania kopii bezpieczeństwa, Z – pomieszczenie w którym wykonywane są kopie bezpieczeństwa, U – pomieszczenie osób wprowadzających dane, A – pomieszczenie administratora bazy danych
[3](K) – kraty w oknach, (A) – alarm, (W) – wzmocnione drzwi

Załącznik nr 7
do zarządzenia 117/2008

WYKAZ ZBIORÓW PRZETWARZANYCH W INNY SPOSÓB NIŻ ELEKTRONICZNY

LP	Nazwa i numer zbioru	Cel przetwarzania danych	Referat (opis)	Osoby przetwarzające dane	Rodzaj danych	Pomieszczenie przetwarzania danych
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						

.....
ABI