WÓJT GMINY POCZESNA
ul. Wolności 2
42-262 Poczesna

Załącznik nr 3 do
Zarządzenia nr 0151/169/09
Wójta Gminy Poczesna
z dnia 12 marca 2009r.

INSTRUKCJA POSTĘPOWANIA W SYTUACJACH NARUSZENIA OCHRONY DANYCH OSOBOWYCH W URZĘDZIE GMINY POCZESNA.

1. Ogólne zasady bezpieczeństwa

Nad bezpieczeństwem przetwarzania danych osobowych w Urzędzie Gminy Poczesna czuwa Administrator Bezpieczeństwa Informacji wyznaczony przez Wójta Gminy Poczesna. Pracownicy zatrudnieni przy przetwarzaniu danych w urzędzie muszą posiadać upoważnienie imienne od Administratora Danych.

Administrator Bezpieczeństwa Informacji zobowiązany jest prowadzić ewidencję przypadków naruszeń bezpieczeństwa przetwarzanych danych celem dokonywania ich analizy oraz wnioskowania do Administratora Danych o udoskonalenie zabezpieczeń fizycznych, systemów operacyjnych lub użytkowych albo zmianę w odpowiednich instrukcjach zarządzania systemami.

Zasadnicze zadania zabezpieczeń bazy danych programów eksploatowanych w urzędzie to ochrona danych osobowych obywateli zamieszkujących na terenie działania Urzędu Gminy Poczesna, czyli mieszkańców gminy Poczesna oraz pracowników urzędu przed nieupoważnionym dostępem, gwarancja poufności przetwarzania danych osobowych, a także umożliwienie obywatelowi dostępu do gromadzonych danych w zakresie przewidzianym przez Ustawę o ochronie danych osobowych (jedn. tekst. Dz. U. z 2002r. nr 101, poz. 926).

System zabezpieczeń w Urzędzie Gminy Poczesna powinien obejmować:
- fizyczne zabezpieczani pomieszczeń, w których wykonywane s ą prace p rzy przetwarzaniu danych osobowych
- zabezpieczenia eksploatowanych systemów operacyjnych,
- zabezpieczenia aplikacji i bazy danych przed nieupoważnionym dostępem

2. Postępowanie w przypadku próby nieuzasadnionego dostępu do danych osobowych

W razie stwierdzenia stanu naruszenia zabezpieczeń pomieszczeń pracownicy muszą natychmiast powiadomić Administratora Bezpieczeństwa Informacji, Administratora Danych oraz Policję (podejrzenie włamania do pomieszczeń, w których umieszczony jest sprzęt komputerowy wraz z systemami danych gdzie przetwarzane są dane osobowe.

W razie stwierdzenia próby naruszenia zabezpieczeń systemu informatycznego, na podstawie:
- stanu sprzętu komputerowego - np.: problemy z jego uruchomieniem, brak zasilania, zmiany w sposobie połączeń sprzętu, stwierdzenie próby łączenia sprzętu przez osoby nieupoważnione,
- różnic w funkcjonowaniu systemu operacyjnego - np.: komunikaty o błędach systemu,
- zmiany w konfiguracji systemów, zmiany w zestawie dostępnych funkcji

- różnic w funkcjonowaniu programów użytkowych - np.: problemy z załogowaniem się uprawnionego użytkownika, stwierdzenie konieczności nieuzasadnionej zmiany hasła, brak dostępu lub zmiany w zestawie funkcji programu, informacje o błędach programu, nieprawidłowości w operacjach wykonywanych przez program, nieuzasadnione zwolnienie lub przyspieszenie pracy programu,
- różnic w zawartości zbioru danych - np.: brak lub nadmiar danych, znalezienie błędnych zapisów,
- innych nieprawidłowości w funkcjonowaniu systemów - np.: niespodziewane "zawieszenia" systemu operacyjnego, albo programu użytkowego, trzeba niezwłocznie powiadomić Administratora Bezpieczeństwa Informacji oraz Administratora Danych, albo osobę przez niego upoważnioną. Wymienione osoby zobowiązane są dokonać analizy źródeł obserwowanej sytuacji i podjąć odpowiednie kroki wyjaśniające oraz działania celem uniknięcia podobnych sytuacji w przyszłości.

Gdy ma miejsce uzasadnione podejrzenie, że naruszenie bezpieczeństwa danych osobowych zostało spowodowane przez zaniedbania lub naruszenia dyscypliny pracy należy natychmiast powiadomić Administratora Bezpieczeństwa Informacji (powinien on przedstawić wniosek Administratorowi Danych o przeprowadzenie postępowania wyjaśniającego lub ewentualne ukaranie odpowiedzialnych osób).

WÓJT
mgr inż. Krzysztof Ujma