Zarządzenie Nr11/2009
Wójta Gminy Krzynowłoga Mała
z dnia 2 lutego 2009 r.

w sprawie wyznaczenia Administratora Bezpieczeństwa Informacji w Urzędzie Gminy w Krzynowłodze Małej.

Na podstawie art.36 ust.3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r., Nr 101 poz. 926 z późn. zm.) oraz art.33 ust.3 ustawy z dnia 8 marca 1990 r . o samorządzie gminnym (tekst jednolity Dz. U. z 2001 r., Nr 142 po0z.1591 z późn. zm) zarządzam, co następuje:

§ 1.

1. Wyznaczam z dniem 2 lutego 2009 r.

Pana Krzysztofa Rzeszot
na Administratora Bezpieczeństwa Informacji
w Urzędzie Gminy w Krzynowłodze Małej.

2. Zakres zadań dla Administratora Bezpieczeństa Informacji stanowi załącznik nr 1 do niniejszego zarządzenia.

§ 2.

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
mgr Adam Bacławski

Załącznik Nr 1 do Zarządzenia
Nr /2009 Wójta Gminy
Krzynowłoga Mała z dnia
2 lutego 2009 r.

Zakres zadań Administratora Bezpieczeństwa Informacji w Urzędzie Gminy w Krzynowłodze Małej

Do zadań Administratora Bezpieczeństwa Informacji należy:

1. Stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy, utratą, uszkodzeniem lub zniszczeniem, oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń poprzez:
   1) Nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe oraz kontrolą przebywających w nich osób,
   2) Prowadzenie szkoleń przed dopuszczeniem do obsługi systemu informatycznego w zakresie przepisów o ochronie danych osobowych oraz wynikających z nich zadań oraz obowiązków,
   3) Prowadzenie okresowych szkoleń stosownie do potrzeb wynikających ze zmian w systemie informatycznym (wymiana sprzętu na nowszej generacji, zmiana oprogramowania) oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmianą wewnętrznych regulacji,
   4) Ustalanie i przydzielanie identyfikatorów zmian dla użytkowników upoważnionych do przetwarzania danych osobowych w systemie informatycznym oraz prowadzenie ewidencji użytkowników,
   5) Zarządzanie hasłami uzytkowników zgodnie z wytycznymi zawartymi w instrukcji określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji,
   6) Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe,
   7) Nadzór nad wykonywaniem kopii awaryjnych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu,
   8) Nadzór czynności związanych ze sprawdzaniem systemu pod kątem obecności wirusów komputerowych w/g instrukcji zarządzania systemem informatycznym,
   9) Nadzór nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących do przetwarzania danych osobowych oraz wszystkimi innymi czynnościami wykonywanymi na bazach danych osobowych,
   10) Nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji,
   11) Nadzór nad obiegiem oraz przechowywaniem dokumentów i wydawnictw zawierających dane osobowe generowane przez system informatuyczny,
   12) Podjęcie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu informatycznego, informacji o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa wg instrukcji postępowania w sytuacji naruszenia danych osobowych,
   13) Analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych (jeśli takie wystąpiło) i przygotowanie oraz przedstawienie administratorowi danych propozycji odpowiednich zmian do instrukcji zarządzania

systemem informatycznym, służącym do przetwarzania danych osobowych.

2. Prowadzenie dokumentacji opisującej sposób przetwarzania danych oraz środki , o których mowa w pkt 1.
3. Kontrola dotycząca, kiedy i przez kogo zostały dane osobowe do zbioru wprowadzone oraz komu są przekazywane.
4. Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych oraz dokonywanie zmian w zakresie przyznanych uprawnień.
5. Zgłaszanie zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych oraz zmiany informacji w zgłoszonym zbiorze danych.

WÓJT

mgr Adam Bacławski