WÓJT GMINY POCZESNA
ul. Wolności 2
42-262 Poczesna

Załącznik nr 1 do
Zarządzenia nr 0151/169/09
Wójta Gminy Poczesna
z dnia 12 marca 2009r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM, SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

Art.36 ustawy o ochronie danych osobowych oraz § 3 ust.1 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. (Dz. U. z 2004r. Nr 100, poz.1024) nakłada obowiązek posiadania i wdrożenia do użytkowania niniejszej instrukcji.

Wszystkie osoby będące w posiadaniu lub wykonujące czynności związane z przetwarzaniem danych osobowych zobowiązane są do stosowanie niniejszej instrukcji.

1) Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;

a) każdy użytkownik systemu informatycznego posiada odrębny identyfikator,
b) identyfikator wpisuje się do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych wraz z imieniem i nazwiskiem użytkownika oraz rejestruje w systemie informatycznym,
c) identyfikator użytkownika pozostaje niezmieniony, a po jego wykorzystaniu nie jest przydzielany innej osobie,
d) w sytuacji gdy osoba utraci uprawnienia do dostępu do danych osobowych, identyfikator tej osoby niezwłocznie wyrejestrowuje się z systemu informatycznego, w którym są one przetwarzane, oraz zakazuje się jej dostępu do danych osobowych,
e) osobą odpowiedzialną za rejestrowanie i wyrejestrowanie użytkowników jest administrator bezpieczeństwa informacji.

2) Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;

a) każdy użytkownik systemu informatycznego wraz z identyfikatorem otrzymuje hasło, które składa się przynajmniej z 6 znaków,
b) hasło użytkownika zmieniane jest co 30 dni, w przypadku wygaśnięcia hasła po wskazanym okresie użytkownik zobowiązany jest do uzyskania nowego hasła od administratora bezpieczeństwa informacji,
c) hasło użytkownika należy utrzymać w tajemnicy również po upływie jego ważności,
d) hasło powinno być przechowywane w postaci zaszyfrowanej,
e) w sytuacji gdy osoba utraci uprawnienia do dostępu do danych osobowych wygasa również hasło.

3) Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;

a) w celu uruchamiania systemu informatycznego należy podać identyfikator i hasło,
b) na każdym stanowisku komputerowym użytkownik zobowiązany jest do ustawienia wygaszacza ekranu tak aby w sytuacji tymczasowego zaprzestania pracy osoby niepowołane nie miały dostępu do danych osobowych,
c) w celu wyrejestrowania się z systemu informatycznego należy zakończyć pracę komputera bądź programu tak aby jego ponowne uruchomienie wymagało podania identyfikatora i hasła
d) niedopuszczalne jest aby przy stanowisku komputerowym przebywały osoby postronne nieposiadające upoważnień do przetwarzania danych, a odpowiedzialność za naruszenia w tym zakresie ponosi kierownik referatu,
e) w sytuacji podejrzenia naruszenia bezpieczeństwa należy zgłosić fakt ten swojemu bezpośredniemu przełożonemu lub kierownikowi zakładu pracy, zastosować środki uniemożliwiające dalszą pracę systemu, zastosować niezbędne środki mające na celu ochronę danych i przeciwdziałanie pogłębiania się skutków zdarzenia, zabezpieczyć dowody mogące posłużyć wyjaśnieniu okoliczności zdarzenia.

4) Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;

a) kopie awaryjne tworzy się poprzez zapisanie danych na dodatkowych dyskietkach, w zależności od potrzeb programu,
b) urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, zabezpiecza się przed utratą w przypadku awarii zasilania lub zakłóceń w sieci poprzez automatyczne tworzenie kopii zapasowych,
c) urządzenia, dyski lub inne elektroniczne nośniki informacji, 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;
- przekazania podmiotowi nieuprawnionemu do przetwarzania danych - pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
- naprawy - pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

5) Sposób, miejsce i okres przechowywania:
- elektronicznych nośników informacji zawierających dane osobowe,
- kopii zapasowych, o których mowa w pkt. 4 ,
a) kopie awaryjne są sprawdzane pod kątem dalszej ich przydatności do odtworzenia danych w przypadku awarii systemu raz na sześć miesięcy,
b) kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;
c) kopie zapasowe usuwa się niezwłocznie po ustaniu ich użyteczności.

6) Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt. III ppkt 1 załącznika do rozporządzenia;

a) system informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:
- działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
- utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

b) możliwe źródła przedostawania się tego typu programów:
- Internet,
- dyskietki i płyty kompaktowe pochodzące z niesprawdzonych źródeł

c) systemy informatyczne zabezpiecza się programami antywirusowymi, które powinny być aktualizowane przez użytkowników.

7) Sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji;

system informatyczny stosowany w Urzędzie Gminy służący do przetwarzania danych osobowych jest ograniczony wyłącznie do edycji tekstu w celu udostępnienia go na piśmie

8) Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

a) przeglądy i konserwacje systemu będą wykonywane raz w miesiącu w celu zmniejszenia zagrożenia przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem danych osobowych

b) osobą wykonującą przeglądy i konserwacje będzie pracownik wskazany przez administratora bezpieczeństwa informacji

c) w przypadku wykonywania przeglądów i konserwacji przez osoby nieposiadające upoważnień do przetwarzania danych, użytkownik przed przystąpieniem do w/w czynności jest zobowiązany powiadomić o tym fakcie administratora bezpieczeństwa informacji, a następnie administrator wyznacza osobę nadzorującą wykonywane prace.

WÓJT
mgr inż. Krzysztof Ujma