Do zapoznania się z niniejszym dokumentem oraz stosowania zawartych w nim zasad zobowiązani są wszyscy pracownicy urzędu upoważnieni do przetwarzania danych osobowych.

Załącznik Nr 2 do Zarządzenia Nr 208/2012
Wójta Gminy Janów
z dnia 26 marca 2012 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI W URZĘDZIE GMINY W JANOWIE

I. Procedury nadawania i zmiany uprawnień do przetwarzania danych.

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych jest zobowiązany do zapoznania się z:
    - Ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych,
    - Polityką bezpieczeństwa informacji w Urzędzie Gminy w Janowie i jednostkach podległych,
    - Instrukcją zarządzania systemami informatycznymi w Urzędzie Gminy w Janowie i jednostkach podległych.
2. Administrator Bezpieczeństwa Informacji przyznaje uprawnienia w zakresie dostępu do systemu informatycznego.
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 tajemnicy. Tajemnica obowiązuje go również po ustaniu zatrudnienia.
9. Odebranie uprawnień pracownikowi następuje na pisemny wniosek kierownika, któremu pracownik podlega z podaniem daty oraz przyczyny odebrania uprawnień.
10. Kierownicy komórek organizacyjnych zobowiązani są pisemnie informować Administratora Bezpieczeństwa Informacji o wszelkich zmianach kadrowych mających wpływ na zakres posiadanych uprawnień w systemie informatycznym.
11. Identyfikator osoby, która utraciła uprawnienia dostępu do danych osobowych należy niezwłocznie wyrejestrować z systemu informatycznego oraz unieważnić jej hasło.
12. Administrator Bezpieczeństwa Informacji zobowiązany jest do prowadzenia rejestru użytkowników i ich uprawnień w systemie informatycznym.
13. Rejestr użytkowników i ich uprawnień w systemie informatycznym, powinien zawierać:
    - imię i nazwisko użytkownika systemów informatycznych,
    - rodzaj uprawnienia,
    - datę nadania uprawnienia,
    - datę odebrania uprawnienia,
    - przyczynę odebrania uprawnienia,
    - podpis Administratora Bezpieczeństwa Informacji.

II. Zasady posługiwania się hasłami.

1. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
2. Hasło użytkownika powinno być zmieniane co najmniej raz na trzy miesiące.
3. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.
4. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł.
5. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
6. Hasło należy wprowadzić w sposób, który uniemożliwia innym osobom jego poznanie.

7. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła.

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

1. Przed rozpoczęciem pracy w systemie komputerowym należy zalogować się do systemu przy użyciu indywidualnego identyfikatora oraz hasła.
2. Po opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wyjść z programu.
3. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów oraz wykonać zamknięcie.
4. Niedopuszczalne jest zamknięcie komputera przed zamknięciem oprogramowania.

IV. Zasady instalacji oprogramowania.

1. Dopuszcza się instalację na serwerze nowego oprogramowania do przetwarzania danych osobowych lub aktualizacji istniejących pod warunkiem spełnienia określonych wymagań.
2. Instalacji oprogramowania lub aktualizacji dokonuje Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona, odnotowuje ten fakt w prowadzonym dzienniku prac systemu.
3. Na wszystkich komputerach Urzędu Gminy w Janowie i jednostkach podległych dopuszcza się instalację tylko legalnego, licencjonowanego oprogramowania.
4. Dopuszczone do zainstalowania programy użytkowe do przetwarzania danych osobowych obejmuje odrębny rejestr.
5. Zabrania się instalowania oprogramowania bez zgody Administrator Bezpieczeństwa Informacji.

V. Procedury tworzenia zabezpieczeń.

1. Za systematyczne przygotowanie kopii bezpieczeństwa odpowiada Administrator Systemu Informatycznego.
2. Kopie bezpieczeństwa wykonywane są w systemie dziennym na dysk twardy narastająco do 30 dni oraz raz na miesiąc na nośnik zewnętrzny.

3. Nośniki z kopiami bezpieczeństwa przechowywane są w przystosowanych do tego szafach.
4. Na każdym stanowisku komputerowym oraz serwerze zainstalowane jest oprogramowanie antywirusowe pracujące w trybie monitora.
5. Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym.
6. Zabrania się pobierania plików niewiadomego pochodzenia z Internetu.
7. Administrator Systemu Informatycznego przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach – minimum raz na kwartał.

VI. Zasady dokonywania napraw.

1. Dokonywanie napraw, przeglądów i konserwacji systemu przez pracowników serwisu mogą odbywać się jedynie w obecności Administratora Bezpieczeństwa Informacji lub osoby przez niego upoważnionej.
2. Przeglądów należy dokonywać nie rzadziej niż raz na kwartał.
3. Fakt dokonania naprawy, przeglądów lub konserwacji musi być udokumentowany w dokumentacji systemu.
4. Uszkodzone nośniki magnetyczne lub inne zawierające dane osobowe nie mogą być użytkowane. Muszą być odpowiednio zabezpieczone przed nieuprawnionym udostępnieniem, a następnie zniszczone lub naprawione pod nadzorem osoby upoważnionej przez Administratora Danych.

VII. Papierowe nośniki danych - wydruki.

1. W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym.
2. Pomieszczenie, w którym przechowywane są wydruki robocze musi być należycie zabezpieczone po godzinach pracy.
3. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

VIII. Profilaktyka antywirusowa.

1. Każdy użytkownik komputera w Urzędzie Gminy w Janowie i jednostkach podległych zobowiązany jest do używania w pracy płyt CD zakupionych przez urząd lub jednostkę podległą (nigdy prywatnych).
2. Informacje i dane przechowywane na płytach CD i pendrivach mogą mieć wyłącznie charakter związany z pracą.
3. Każdy komputer minimum raz w tygodniu powinien zostać sprawdzony aktualną wersją programu antywirusowego.
4. Płyty CD i pendrivy przekazywane Urzędowi gminy lub jednostkom podległym mogą być odczytywane na komputerach, tylko i wyłącznie po wcześniejszym sprawdzeniu programem antywirusowym.

IX. Zasady korzystania z Internetu.

Przy korzystaniu z Internetu w Urzędzie Gminy w Janowie i jednostkach podległych należy stosować następujące zasady:

1. Pracownicy mogą korzystać z dostępu do Internetu tylko i wyłącznie w celach służbowych, tj. w zakresie:
   a) poszukiwania wyjaśnień i interpretacji przepisów prawnych,
   b) komunikacji i pozyskiwania informacji z innych urzędów administracji rządowej jak i samorządowej wynikające z wykonywanych obowiązków służbowych,
   c) przeglądania stron – Biuletynów Informacji Publicznej prowadzonych w oparciu o przepisy ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. Nr 112, poz. 1198 z późn. zm.),
   d) kopiowania danych wykorzystywanych wyłącznie do celów służbowych o ile nie jest to sprzeczne z prawem autorskim.

2. Niedozwolone jest:
   a) kopiowanie na dysk twardy komputera danych oraz instalacji programów dostępnych na serwerach internetowych,
   b) użytkowanie jakichkolwiek programów niezwiązanych z wykonywanymi obowiązkami służbowymi,

c) odwiedzanie popularnych serwisów i wszystkich innych stron (np. Nasza klasa, Facebook, Allegro, Ceneo, itp.), które nie zawierają treści pomocnych przy wykonywaniu obowiązków służbowych,
d) realizacji swoich własnych spraw, np. (zakupy, wysyłanie osobistych e-maili z własnych skrzynek pocztowych, dokonywanie przelewów (płatności) z rachunków osobistych),
e) grania w popularne gry dostępne w Internecie.