WÓJT GMINY
BOJANÓW
ul. Parkowa 5, 37-433 Bojanów
woj. podkarpackie

**Zarzadzenie_Nr_53 _2010**
**Wójta Gminy Bojanów**
**Z dnia 1 września 2010 roku**

**w sprawie wprowadzenia polityki bezpieczeństwa danych osobowych w Urzędzie Gminy Bojanów**

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 roku Nr 101, poz.926 z późn., zm.) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych ( Dz. U. Nr 100, poz. 1024) oraz w związku z art.33 ust.1 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym ( Dz. U. z 2001 roku Nr 142, poz.1591 z późn. zm.)

**zarządza co następuje**

**§ 1**

Wprowadza się politykę bezpieczeństwa danych osobowych w Urzędzie Gminy Bojanów stanowiącą załącznik do zarządzenia.

**§ 2**

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
*Sławomir Serafin*

Załącznik
do Zarządzenia Nr 53 / 2010
Wójta Gminy Bojanów
z dnia 1 września 2010 r.

# Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Bojanów

# WPROWADZENIE

Niniejszy dokument jest zgodny z następującymi aktami prawnymi:

1) ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity Dz.U. Nr 101, z 2002r., poz. 926,
2) rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024).

Niniejszy dokument reguluje sprawy ochrony danych osobowych zawartych w systemie informatycznym w lokalnej sieci komputerowej oraz zbiorów danych zapisanych w postaci dokumentacji papierowej w Urzędzie Gminy Bojanów
Obszar przetwarzania danych osobowych stanowią części pomieszczeń nr: 1, 3, 8, 10, 12, 13, 14, 15, 16.

Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę Urzędu. Dokument zwraca uwagę na konsekwencje, jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

Odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi współczesnym systemom informatycznym. Dokument „Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Bojanów", zwany dalej „Polityką bezpieczeństwa", wskazujący sposób zabezpieczenia systemów informatycznych postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w systemach informatycznych, przeznaczony jest dla osób zatrudnionych przy przetwarzaniu tych danych.

Potrzeba jego opracowania wynika z §3 rozporządzenia Prezesa Rady Ministrów z dnia 25 lutego 1999r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz.U. Nr 18, poz. 162) oraz §3 i 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024).

1) „Polityka bezpieczeństwa" określa tryb postępowania w przypadku, gdy:
   - stwierdzono naruszenie zabezpieczeń systemu informatycznego,
   - stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci informatycznej mogą wskazywać na naruszenie zabezpieczeń tych danych.
2) „Polityka bezpieczeństwa" obowiązuje wszystkich pracowników Urzędu Gminy Bojanów. Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemie informatycznym Urzędu.

3) Administratorem Danych jest Wójt Gminy Bojanów. Administrator Danych swoją decyzją wyznacza Administratora Bezpieczeństwa Informacji danych zawartych w systemach informatycznych Urzędu, zwanego dalej „Administratorem Bezpieczeństwa".

4) „Administrator Bezpieczeństwa" realizuje zadania w zakresie ochrony danych, a w szczególności:
   - ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Urzędu,
   - podejmowania stosownych działań zgodnie z niniejszą „Polityką bezpieczeństwa" w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym,
   - niezwłocznego informowania Administratora Danych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
   - nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych.

## Rozdział 1

# OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

1) Podział zagrożeń:

- zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych,
- zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora systemu, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych,
- zagrożenia zamierzone, świadome i celowe – najpoważniejsze zagrożenia, naruszenie poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nie uprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

2) Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:

- sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: pożar, zalanie pomieszczeń, katastrofa budowlana itp.;
- niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego,
- awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych, a także niewłaściwe działanie serwisu,
- pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
- jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
- nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
- stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
- nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,

- ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony danych osobowych albo inne strzeżone elementy systemu zabezpieczeń,
- praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych – np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
- ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki", itp.,
- podmieniono lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe,
- rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

3) Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej itp.

## Rozdział 2

# ZABEZPIECZENIE DANYCH OSOBOWYCH

### §1.
### Cele i zasady ogólne

1) Administratorem danych osobowych zawartych i przetwarzanych w systemach informatycznych Urzędu Gminy jest Wójt.

2) Administrator danych osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych Urzędu, a w szczególności:

- zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
- zapobiegać zabraniu danych przez osobę nieuprawnioną,
- zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.

### §2.
### Cele i zasady ochrony danych

1) Celem wprowadzonych niniejszą „Polityką bezpieczeństwa" jest ochrona danych osobowych zawartych w systemie Urzędu. Określone niżej sposoby zabezpieczeń dotyczą:

1.1. zabezpieczeń przed dostępem do danych osób nieupoważnionych na etapie eksploatacji systemu, tj. wprowadzanie danych, aktualizacji lub usuwania danych, wyświetlania lub drukowania zestawień,
1.2. ochrony danych zarchiwizowanych na nośnikach zewnętrznych, procedur niszczenia niepotrzebnych wydruków lub nośników danych,
1.3. systemu zabezpieczeń przed dostępem osób niepowołanych do pomieszczeń, w których są eksploatowane urządzenia oraz sposobów dostępu do tych pomieszczeń pracowników, personelu pomocniczego Urzędu oraz serwisu zewnętrznego,
1.4. zakresu obowiązków pracowników – w części dotyczącej bezpieczeństwa danych.

2) Strategia ochrony danych osobowych opiera się na następujących zasadach:

2.1. fizyczny dostęp do pomieszczeń, w których znajdują się systemy informatyczne blokują drzwi i systemy alarmowe,
2.2. podstawowym sposobem zabezpieczenia danych i dostępu do nich jest system definiowania użytkowników oraz haseł, uniemożliwiający dostęp do systemu osobom nieupoważnionym,
2.3. kopie danych zarchiwizowanych na nośnikach magnetycznych lub płytach CD są przechowywane w metalowej szafie, w pomieszczeniu zgodnym z Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać

urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024), znajdującym się w budynku Urzędu, w pokoju nr 4,

2.4. w pomieszczeniach, w których zainstalowany jest serwer i komputery zawierające bazy danych są zainstalowane systemy alarmowe i przeciwpożarowe,

2.5. za całość Polityki Bezpieczeństwa odpowiada Administrator Bezpieczeństwa.

## §3.
## Zabezpieczenia

Wprowadza się następujące zabezpieczenia danych w systemie informatycznym:

1) Na wszystkich stacjach roboczych, na których przetwarzane są dane osobowe wprowadza się **wysoki** poziom zabezpieczeń.
2) Pomieszczenia, w których stoi serwer i komputery zawierające dane osobowe i kartoteki osobowe są zabezpieczone poprzez system alarmowy i przeciwpożarowy.
3) Ochronę przed awariami zasilania oraz zakłóceniami w sieci energetycznej serwera i stacji roboczych zapewniają zasilacze UPS.
4) Uruchomienie stacji roboczych, na których przetwarzane są dane osobowe wymaga podania hasła BIOS-u.

   4.1. hasło każdego użytkownika jest unikalne, składające się co najmniej z 6 znaków, zawiera małe i duże litery, cyfry oraz znaki specjalne,

   4.2. hasła przechowywane są w wyznaczonym pomieszczeniu zwanym dalej „Serwerownią", znajdującym się w budynku Urzędu na parterze, w metalowej szafie, w zamkniętych kopertach, na specjalnym druku stanowiącym **załącznik 1** do niniejszego dokumentu,

   4.3. dostęp do haseł posiada Administrator Danych oraz Administrator Bezpieczeństwa,

   4.4. hasła zmieniane są nie rzadziej niż co 60 dni. Zmiana haseł następuje w pierwszym tygodniu, nie później niż do 10 dnia każdego miesiąca, w obecności Administratora Bezpieczeństwa.

   4.5. w przypadku nieobecności Administratora Systemu, osoba zastępująca protokołem przekazania (**załącznik 2**) w obecności Administratora Bezpieczeństwa odbiera hasło dostępu, po czym zmienia je na własne różniące się znacznie od poprzedniego,

   4.6. hasła są przechowywane przez okres 30 dni od zmiany, po czym następuje zniszczenie w obecności Administratora Danych oraz Administratora Bezpieczeństwa.

   4.7. za prowadzenie ewidencji haseł odpowiada Administrator Bezpieczeństwa.

5) Oprogramowanie wykorzystywane do przetwarzania danych posiada własny system kont (zabezpieczonych hasłami) i uprawnień.
6) Administrator Systemu wykorzystujący oprogramowanie o którym jest mowa w pkt 5, przekazuje hasło i login do aplikacji Administratorowi Bezpieczeństwa w zamkniętej kopercie, która jest przechowywana w pomieszczeniu z pkt 4.2.
7) Hasło w pkt 4 musi być różne od hasła w pkt 5.
8) W przypadku ujętym w pkt 4.5, instrukcje stosuje się odpowiednio.

9) W celu ochrony przed dostępem do danych komputera z sieci publicznej wykorzystuje się system zapory ogniowej dostępnej na Routerze dostępowym.
10) Stosuje się aktywną ochronę antywirusową w czasie rzeczywistym na każdym komputerze podłączonym do sieci publicznej. Za aktualizację bazy wirusów odpowiada Administrator Bezpieczeństwa.
11) Wydruki zawierające dane osobowe powinny znajdować się w miejscu, które uniemożliwia dostęp osobom postronnym.
12) Kopie bezpieczeństwa na nośnikach optycznych wykonywane są okresowo w ramach swoich obowiązków, nie rzadziej niż co 6 miesięcy. Kopie bezpieczeństwa przechowywane są w kasie pancernej w „Serwerowni". Dostęp do nośników zawierających kopie mają tylko uprawnione osoby.
13) Kartoteki papierowe znajdują się w meblowych szafach, zamykanych na zamki meblowe w pokojach, w których przetwarzane są dane osobowe.
14) Dostęp do danych mają wyłącznie pracownicy wyznaczeni przez Administratora Danych.

## §4.
## Szkolenia

1) Szkolenie podstawowe dotyczące bezpieczeństwa danych obejmuje wszystkich pracowników Urzędu Gminy.
2) Szkoleniem szczegółowym obejmuje się pracowników zatrudnionych bezpośrednio przy przetwarzaniu danych, w tym danych osobowych.
3) Tematyka szkoleń obejmuje:

   a) Przepisy i instrukcje wewnętrzne dotyczące ochrony danych, archiwizacji zasobów i przechowywania nośników, niszczenie wydruków i zapisów na nośnikach magnetycznych i optycznych,
   b) Zakresy obowiązków pracowników związanych bezpośrednio z bezpieczeństwem danych i ochroną systemów na poszczególnych stanowiskach.

## §5.
## Archiwizowanie danych

1) Administrator systemu wykonuje raz w tygodniu kopie zapasowe zapisane w programie, oraz kopie bezpieczeństwa nie rzadziej niż co 6 miesięcy.
2) Kopie zapasowe przechowywane są w miejscu pracy, zaś kopie bezpieczeństwa w „Serwerowni".
3) Dyskietki, na których zapisywane są kopie zapasowe oraz kopie bezpieczeństwa są każdorazowo wymazywane i formatowane, w taki sposób, aby nie można było odtworzyć ich zawartości. Płyty CD niszczy się trwale w sposób mechaniczny.
4) Okresową weryfikację kopii bezpieczeństwa pod kątem ich przydatności do odtworzenia danych przeprowadza Administrator Bezpieczeństwa.

## §6.
## Niszczenie wydruków i zapisów na nośnikach magnetycznych

1) Nośniki magnetyczne przekazywane na zewnątrz powinny być pozbawione zapisów zawierających dane osobowe. Niszczenie poprzednich zapisów odbywa się poprzez wymazywanie informacji oraz formatowanie nośnika.
2) Poprawność przygotowania nośnika magnetycznego jest sprawdzana przez Administratora Bezpieczeństwa.
3) Uszkodzone nośniki magnetyczne przed ich wyrzuceniem są fizycznie niszczone.
4) Po wykorzystaniu wydruki zawierające dane osobowe są niszczone w specjalnym urządzeniu znajdującym się w budynku Urzędu.

## Rozdział 3

# POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1) Każdy pracownik Urzędu Gminy , który poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe bądź posiada informacje mogącą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany fakt ten niezwłocznie zgłosić Administratorowi Bezpieczeństwa.
2) W razie niemożności zawiadomienia Administratora Bezpieczeństwa lub osoby przez niego upoważnionej, należy powiadomić bezpośredniego przełożonego.
3) Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Bezpieczeństwa lub upoważnionej przez niego osoby, należy:

    - niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
    - rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
    - zaniechać – o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
    - podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
    - podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
    - zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
    - udokumentować wstępnie zaistniałe naruszenie,
    - nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa lub osoby upoważnionej.

4) Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Administrator Bezpieczeństwa lub osoba go zastępująca:

    - zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Urzędu,
    - może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
    - rozważa celowość i potrzebę powiadomienia o zaistniałym naruszeniu Administratora danych,
    - nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza Urzędu.

5) Administrator Bezpieczeństwa dokumentuje zaistniały przypadek naruszenia oraz sporządza raport, który powinien zawierać w szczególności:

- wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
- określenie czasu i miejsca naruszenia i powiadomienia,
- określenie okoliczności towarzyszących i rodzaju naruszenia,
- wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
- wstępną ocenę przyczyn wystąpienia naruszenia,
- ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

6) Raport, o którym mowa w pkt 5, Administrator Bezpieczeństwa niezwłocznie przekazuje Administratorowi Danych, a w przypadku jego nieobecności osobie uprawnionej.
7) Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu Administrator Bezpieczeństwa zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzanych danych.
8) Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Administratora Danych, Administratora Bezpieczeństwa, Pełnomocnika ds. Ochrony Informacji Niejawnych.
9) Analiza powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

## Rozdział 4

## POSTANOWIENIA KOŃCOWE

1) Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.
2) Administrator Bezpieczeństwa zobowiązany jest prowadzić ewidencję osób , które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych.
3) Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym Administratora Bezpieczeństwa.
4) Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia Administratora Bezpieczeństwa nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
5) W sprawach nieuregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych, Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024), oraz Rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004r. w sprawie sposobu technicznego przygotowania systemów i sieci do przekazywania informacji – do gromadzenia wykazów i połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczenia danych informatycznych (Dz.U. Nr 100, poz. 1023).

**Załącznik Nr 1**
do „Polityki bezpieczeństwa
i instrukcji zarządzania systemem informatycznym
służącym do przetwarzania danych osobowych
w Urzędzie Gminy Bojanów

**Komórka: .....**

## HASŁO DOSTĘPU DO SYSTEMU:

| |
|---|
| |

Pieczęć i podpis użytkownika:

Administrator Bezpieczeństwa:

**Załącznik Nr 2**
do „Polityki bezpieczeństwa
i instrukcji zarządzania systemem informatycznym
służącym do przetwarzania danych osobowych
w Urzędzie Gminy Bojanów

# PROTOKÓŁ PRZEKAZANIA HASŁA DOSTĘPU DO SYSTEMU

**Osoba przekazująca:**

**komórka: .....**

**data przekazania i podpis: .....**

**w obecności : .....**

**przekazała hasło dostępu w zamkniętej kopercie:**

**Osobie przyjmującej:**

**komórka .....**

**podpis odbierającego: .....**