ZARZĄDZENIE Nr 53/06
BURMISTRZA GMINY ZAKROCZYM

z dnia 20.11.2006r

w sprawie: dokumentacji przetwarzania danych osobowych w Urzędzie Gminy w Zakroczmiu.

Na podstawie § 3. Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. 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. z dnia 1 maja 2004 r.) zarządza się co następuje:

§ 1

Wprowadza się do stosowania w Urzędzie Gminy „Politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

§ 2

Wykonanie zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§ 3

Traci moc zarządzenie Nr 21/01 Burmistrza Gminy Zakroczym z dnia 9.11.2001 r. w sprawie ochrony danych osobowych w Urzędzie Gminy w Zakroczmiu.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ GMINY

Henryk Ruszczyk

URZĄD GMINY W ZAKROCZYMIU

POLITYKA BEZPIECZEŃSTWA
I
INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM
w Urzędzie Gminy w Zakroczymiu

Opracował:
Pełnomocnik ds. Ochrony Informacji Niejawnych
Bogumił HORODECKI

ZAKROCZYM
2006

SPIS TREŚCI:

URZĄD GMINY W ZAKROCZYMIU

POLITYKA BEZPIECZEŃSTWA DANYCH SOBOWYCH URZĘDU GMINY W ZAKROCZYMIU

ZAKROCZYM

2006

WPROWADZENIE

Niniejszy dokument określa zakres czynności niezbędnych do wykonania oraz reguły ich wdrażania i stosowania dla zapewnienia bezpieczeństwa danych osobowych przetwarzanych w Urzędzie.

Dokument określa procedury postępowania użytkowników systemów informatycznych w Urzędzie w działaniu codziennym oraz w sytuacji zagrożeń, ich obowiązki a także konsekwencje, jakie mogą ponosić osoby nie przestrzegające obowiązujących przepisów.

Administratorem danych osobowych w Urzędzie Gminy w Zakroczymiu jest Burmistrz Gminy, który wyznacza **Administratora Bezpieczeństwa Informacji**, zwanego dalej **ABI.**

Ustalenia zawarte w niniejszym dokumencie obowiązują wszystkich pracowników Urzędu Gminy przetwarzających lub mających dostęp do danych osobowych Urzędu.

Podstawę do opracowania dokumentu stanowią następujące akty prawne:

1. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 i Nr 1534, poz. 1271 oraz z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285)
2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. 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. 04.100.1024 z dnia 1 maja 2004 r.).
3. Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U. Nr 11, poz. 95 z późn. zm.).

1. OPIS ZDARZEŃ NARUSZAJĄCYCH BEZPIECZEŃSTWO DANYCH OSOBOWYCH

1.1. **Zagrożenia losowe zewnętrzne** (klęski żywiołowe np. pożar, niezapowiedziane przerwy w zasilaniu) – mogą prowadzić do utraty integralności danych lub ich zniszczenia, uszkodzenia infrastruktury technicznej systemu, zakłócenia jego ciągłości – nie dochodzi do naruszenia poufności danych.

1.2. **Zagrożenia losowe wewnętrzne** (niezamierzone pomyłki operatorów, awarie sprzętowe, błędy oprogramowania itp.) – może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu – może nastąpić naruszenie poufności danych.

1.3. **Zagrożenia zamierzone, świadome i celowe** (najgroźniejsze) – następuje naruszenie poufności danych, zazwyczaj bez uszkodzenia infrastruktury technicznej i zakłócenia ciągłości pracy systemu. Zagrożenia te to:

- nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu);
- nieuprawniony dostęp do systemu z jego wnętrza;
- nieuprawniony przekaz danych;
- pogorszenie jakości sprzętu i oprogramowania;
- bezpośrednie zagrożenie materialnych składników systemu.

2. ZABEZPIECZENIE DANYCH OSOBOWYCH

2.1. Administrator danych zarządza zastosowanie **środków technicznych i organizacyjnych** zapewniających ochronę przetwarzanych w Urzędzie danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. Zastosowane środki mają za zadanie zabezpieczyć dane w szczególności przed:

- udostępnieniem ich osobom nieuprawnionym;
- zabraniem przez osobę nieuprawnioną;
- przetwarzaniem z naruszeniem ustawy;
- zmianą, utratą, uszkodzeniem lub zniszczeniem.

2.2. Do zastosowanych w Urzędzie **środków technicznych** należą:

a) przetwarzanie danych osobowych w wydzielonych, odpowiednio przystosowanych do tego i zabezpieczonych pomieszczeniach;
b) szczególne zabezpieczenie centrum przetwarzania danych (serwer) poprzez zastosowanie zaawansowanego systemu kontroli dostępu oraz dedykowanego systemu ochrony p.poż.;

c) wyposażenie pomieszczeń w szafy metalowe, dające gwarancję bezpieczeństwa dokumentacji.

2.3. Do zastosowanych **środków organizacyjnych** należą:

a) zapoznanie każdej osoby przed dopuszczeniem jej do pracy przy przetwarzaniu danych osobowych z przepisami dotyczącymi ochrony danych osobowych i odpowiedzialnością karną i dyscyplinarną za ich nieprzestrzeganie;
b) przeszkolenie osób, o których mowa w p. 1) w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochrona danych osobowych,
c) kontrolowanie pomieszczeń, urządzeń, programów, dokumentacji i sposobu pracy w zakresie przestrzegania zasad ochrony danych.

2.4. Niezależnie od ustaleń zawartych w dokumencie „Polityka Bezpieczeństwa ..." mają zastosowanie wszelkie regulaminy i instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych a także indywidualne zakresy zadań osób zatrudnionych w Urzędzie przy przetwarzaniu danych osobowych. Dokumenty te nie mogą być sprzeczne z uregulowaniami zawartymi w „Polityce Bezpieczeństwa...".

3. KONTROLA PRZESTRZEGANIA ZASAD BEZPIECZEŃSTWA DANYCH OSOBOWYCH

3.1. Nadzór nad przestrzeganie zasad ochrony danych osobowych w Urzędzie sprawuje Administrator Bezpieczeństwa Informacji

3.2. ABI sporządza roczne plany kontroli zatwierdzane przez Burmistrza i zgodnie z nimi przeprowadza kontrole oraz dokonuje oceny stanu bezpieczeństwa danych osobowych w Urzędzie.

3.3. Na podstawie zebranych materiałów ABI sporządza sprawozdanie roczne, które przedstawia Administratorowi danych (Burmistrzowi).

3.4. Administrator Bezpieczeństwa Informacji w nadzorze nad ochroną danych osobowych ściśle współdziała z Pełnomocnikiem Ochrony Informacji Niejawnych.

4. POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

4.1. W przypadku stwierdzenia naruszenia:

- zabezpieczenia systemu informatycznego,
- technicznego stanu urządzeń,
- zawartości zbioru danych osobowych,
- ujawnienia (nieuprawnionego) metody pracy lub sposobu działania programu,

- jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie tych danych,
- innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (zalanie, pożar, itp.)

każda osoba zatrudniona przy przetwarzaniu danych osobowych jest obowiązana niezwłocznie powiadomić o tym fakcie Administratora Bezpieczeństwa Informacji.

4.2. W razie niemożliwości zawiadomienia ABI lub osoby przez niego upoważnionej, należy powiadomić bezpośredniego przełożonego.

4.3. Administrator Bezpieczeństwa Informacji dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg zasad określonych w ***„Instrukcji postępowania w przypadku naruszenia systemu ochrony danych osobowych"***.

4.4. Raport, o którym mowa w ust. 4.3. ABI niezwłocznie przekazuje Burmistrzowi, a w przypadku jego nieobecności osobie uprawnionej.

4.5. Po wyczerpaniu środków doraźnych po zaistniałym przypadku naruszenia ABI zasięga niezbędnych opinii i proponuje postępowanie naprawcze, w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.

4.6. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez kierownictwo Urzędu, Administratora Bezpieczeństwa Informacji, Pełnomocnika ds. Ochrony Informacji Niejawnych i inne zainteresowane osoby.

4.7. Analiza, o której mowa w ust. 6 powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym przypadkom naruszenia w przyszłości.

5. POSTANOWIENIA KOŃCOWE

5.1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu będą traktowane jako ciężkie naruszenia obowiązków pracowniczych. 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 ustalonymi zasadami, a także, gdy nie realizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.

5.2. Orzeczona kara dyscyplinarna nie wyklucza odpowiedzialności karnej ukaranej osoby zgodnie z art. 49 – 54 ustawy o ochronie danych osobowych (tekst jednolity Dz. U. z

2002 r. Nr 101, poz. 926) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

5.3. Osoby, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych, potwierdzają ten fakt przez podpisanie oświadczenia (wzór – załącznik Nr 1 do Instrukcji Ochrony...). Oświadczenia przechowywane są u Administratora Bezpieczeństwa Informacji.

5.4. Wszystkie regulacje dotyczące systemów informatycznych określone w Polityce Bezpieczeństwa mają zastosowanie również przy przetwarzaniu danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.

URZĄD GMINY W ZAKROCZYMIU

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

ZAKROCZYM

2006

I. ZASADY OGÓLNE.

§ 1

Podstawę prawną do opracowania niniejszej instrukcji stanowią:

1. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 833 z późn. zmianami), zwana dalej Ustawą;

2. Rozporządzenie ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r. 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. z dnia 1 maja 2004 r.

§ 2

Instrukcja określa zasady zarządzania systemem informatycznym służącym do przetwarzania danych osobowych , jak również do przetwarzania danych osobowych zawartych w innych zbiorach w Urzędzie Gminy Zakroczym ze szczególnym uwzględnieniem wymogów bezpieczeństwa i ochrony danych osobowych.

§ 3

Przez użyte w Instrukcji określenia należy rozumieć:

- **Dane osobowe** – to każda informacja dotycząca osoby fizycznej, pozwalająca na określenie tożsamości tej osoby;

- **Zbiór (baza) danych** – to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

- **Przetwarzanie danych** – to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie a zwłaszcza te, które wykonuje się w systemach informatycznych;

- **Usuwanie danych** – zniszczenie danych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

- **Administrator danych** – to organ, instytucja, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych – w przypadku Urzędu Gminy jest nim Burmistrz;

- **Zgoda osoby, której dane dotyczą** – to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie – zgoda nie może być domniemana lub dorozumiana z oświadczenia o woli innej treści:

- **Użytkownik** – to osoba upoważniona do dostępu i przetwarzania danych osobowych;

- **System informatyczny** – to system przetwarzania danych w Urzędzie Gminy wraz ze związanymi z nim ludźmi oraz zasobami technicznymi.

§ 4

Administrator danych wyznacza **Administratora bezpieczeństwa informacji (ABI)**, jako osobę odpowiedzialną za bezpieczeństwo danych osobowych w systemach informatycznych, a szczególnie za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarza się dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.

§ 5

Każda osoba przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych wynikającego z indywidualnego zakresu obowiązków powinna być zaznajomiona z przepisami dotyczącymi ochrony danych osobowych, w tym z przepisami karnymi Ustawy. Fakt ten pracownik potwierdza **oświadczeniem** (Wzór – Załącznik Nr 1), a dopuszczenie do pracy uzyskuje na podstawie odpowiedniego **upoważnienia** (Wzór – Załącznik Nr 2). Zaznajomienia pracownika z przepisami dokonuje Pełnomocnik Burmistrza ds. Ochrony Informacji Niejawnych, zwany dalej Pełnomocnikiem Ochrony lub osoba przez niego upoważniona.

§ 6

W razie utworzenia lub likwidacji stanowiska pracy, zmiany zakresu obowiązków pracowniczych, zmiany sposobu przetwarzania danych lub w innych przypadkach, które wpływają bezpośrednio na rodzaj i zakres przetwarzania danych, ABI po uzgodnieniu z Sekretarzem Gminy zobowiązany jest bezzwłocznie skierować do Administratora Danych wniosek o wydanie lub cofnięcie upoważnienia do przetwarzania danych osobowych.

§ 7

Wypowiedzenie umowy o pracę jest równoznaczne z cofnięciem upoważnienia do przetwarzania danych osobowych.

§ 8

Przetwarzanie danych osobowych sprzeczne z Ustawą stanowi naruszenie obowiązków pracowniczych.

§ 9

Osoby zatrudnione przy przetwarzaniu danych osobowych są zobowiązane do zachowania ich w tajemnicy zarówno w czasie zatrudnienia, jak też po jego ustaniu.

§ 10

Administrator danych określa pomieszczenia lub ich części tworzące obszar, w którym przetwarzane są dane osobowe przy użyciu stacjonarnego sprzętu komputerowego (Zał. Nr 3).

§ 11

Budynki lub pomieszczenia, w których przetwarzane są dane osobowe powinny być zamykane w czasie nieobecności w nich osób tam pracujących w sposób uniemożliwiający dostęp osób nieuprawnionych.

§ 12

Osoby nieupoważnione mogą przebywać wewnątrz obszaru określonego w § 11 jedynie w obecności osoby zatrudnionej przy przetwarzaniu danych i za zgodą administratora danych lub osoby przez niego upoważnionej.

§ 13

W pomieszczeniach, w których przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.

§ 14

Dla każdej osoby, której dane są przetwarzane w systemie informatycznym powinno być odnotowane:

1) data pierwszego wprowadzenia do systemu danych tej osoby;

2) źródła pochodzenia danych, jeżeli dane mogą pochodzić z różnych źródeł;

3) identyfikator użytkownika wprowadzającego dane;

4) informacja: komu, kiedy, w jakim zakresie dane zostały udostępnione, jeśli przewidziane jest udostępnianie innym podmiotom, chyba że dane te traktuje się jako dane powszechnie dostępne;
5) żądanie czasowego lub stałego wstrzymania wykorzystywania danych lub ich usunięcie, jeżeli zostały zebrane niezgodnie z prawem lub są już zbędne dla celu ich zebrania.

§ 15

Dane osobowe udostępniane są na pisemny, umotywowany wniosek skierowany do Burmistrza, zawierający informacje umożliwiające wyszukanie w odpowiednim zbiorze żądanych danych oraz wskazujący ich zakres i przeznaczenie.

§ 16

Burmistrz odmawia udostępnienia danych osobowych ze zbioru, gdy mogłoby to spowodować:

1) ujawnienie wiadomości stanowiącej tajemnicę państwową;

2) zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi, mienia lub bezpieczeństwa porządku publicznego;

3) zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa;

4) istotne naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.

§ 17

Jeżeli przepisy innych ustaw, które odnoszą się do przetwarzania danych osobowych, przewidują dalej idącą ich ochronę niż wynika to z niniejszej instrukcji, stosuje się przepisy tych ustaw.

II. INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Nadawanie uprawnień do przetwarzania danych i rejestrowanie tych uprawnień w systemie informatycznym.

§ 1

Każdy użytkownik systemy przed dopuszczeniem do przetwarzania danych osobowych w systemie informatycznym musi odbyć odpowiednie **przeszkolenie**, uzyskać **upoważnienie** do obsługi systemu(Wzór – Załącznik Nr 2) oraz podpisać oświadczenie o zaznajomieniu się z przepisami o ochronie danych osobowych i odpowiedzialności karnej za ich naruszenie (Wzór – Załącznik nr 1).

§ 2

Po spełnieniu warunków określonych w § 1 użytkownik systemu informatycznego otrzymuje identyfikator i zostaje zarejestrowany w systemie.

2. Metody i środki uwierzytelnienia oraz procedury ich zarządzania i użytkowania.

§ 3

Każdy użytkownik systemu informatycznego, w którym przetwarza się dane osobowe otrzymuje ustalony, odrębny **identyfikator i hasło**.

§ 4

Identyfikator użytkownika wpisuję się wraz z imieniem i nazwiskiem do ewidencji użytkowników systemu oraz rejestruje w systemie informatycznym.

§ 5

Identyfikator osoby, która utraciła prawo dostępu do danych osobowych należy niezwłocznie wyrejestrować z danego systemu informatycznego. Osobie takiej należy również unieważnić hasło oraz podjąć inne stosowne działania mające na celu zapobieżenie dalszemu dostępowi tej osoby do danych osobowych.

§ 6

Identyfikator użytkownika jest niezmienny przez cały czas jego pracy w systemie informatycznym Urzędu.

§ 7

Hasło użytkownika powinno być zmieniane co najmniej raz w miesiącu.

§ 8

1.Odpowiedzialnym za nadawanie uprawnień do przetwarzania danych i rejestrowanie tych uprawnień a także przydział identyfikatorów i haseł jest Administrator Bezpieczeństwa Informacji (ABI).

2. W wykonywaniu czynności wymienionych w ust. 1. ABI współdziała z Pełnomocnikiem ochrony informacji niejawnych.

3. Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym.

§ 9

Włączenie systemu powinno odbywać się zgodnie z instrukcją jego obsługi po uprzednim sprawdzeniu, czy urządzenia systemu nie noszą śladów włamania lub nie są uszkodzone.

§ 10

Po zakończeniu przetwarzania danych upoważniony pracownik powinien sporządzić kopię awaryjną.

§ 11

Przed opuszczeniem pomieszczenia w czasie lub po zakończeniu pracy użytkownik systemu informatycznego powinien sprawdzić stan zabezpieczenia urządzeń systemu przed utratą danych lub ich nieuprawnionym udostępnieniem.

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

§ 12

Użytkownicy systemu sporządzają codziennie kopię zbiorów danych przy użyciu programu archiwizującego przez przekopiowanie ich na elektroniczne nośniki informacji (dyskietki, CD) lub do katalogu na dysku twardym. **Codzienne kopie** sporządza się w przypadku, jeśli w ciągu dnia były wprowadzane zmiany w zbiorze danych.

§ 13

Ostatniego dnia tygodnia sporządza się **kopię tygodniową** a ostatniego dnia roboczego miesiąca **kopię miesięczną.**

§ 14

Ostatniego dnia roboczego roku sporządza się **kopię roczną**. Kopia ta wraz z kopiami miesięcznymi archiwizowana jest na CD-ROMie.

5. **Sposób i czas przechowywania nośników informacji zawierających dane osobowe.**

§ 15

Kopie awaryjne nie mogą być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych. Wskazane jest przechowywanie ich w szafie pancernej kancelarii tajnej lub w pomieszczeniu zajmowanym przez ABI.

§ 16

Kopie awaryjne i inne nośniki danych osobowych należy okresowo sprawdzać pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu i bezzwłocznie usuwać po ustaniu ich użyteczności.

§ 17

Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

6. **Zabezpieczenie systemu przed nieuprawnionym dostępem obcych programów oraz utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.**

§ 18

Administrator Bezpieczeństwa Informacji zobowiązany jest raz w miesiącu zapewnić sprawdzenie w systemie obecności wirusów komputerowych – przy użyciu co najmniej jednego programu antywirusowego, umożliwiającego wykrycie i usunięcie wirusów.

§ 19

W przypadku wykrycia wirusa, gdy nie jest możliwe jego usunięcie programem antywirusowym, należy wykasować zarażone programy i ponownie je zainstalować.

§ 20

Urządzenia informatyczne, w których przetwarzane są dane osobowe chronione są przed utratą tych danych spowodowaną awarią sieci zasilającej poprzez podłączenie tych urządzeń do sieci awaryjnej (akumulatorowej).

7. **Sposób postępowania w zakresie komunikacji w sieci komputerowej.**

§ 21

Przesyłanie danych osobowych danych osobowych w sieci komputerowej Urzędu jest możliwe wyłącznie po uzyskaniu zgody administratora danych udzielonej na wniosek ABI.

§ 22

Udostępnianie lub przekazywanie danych poprzez Internet jest w Urzędzie zabronione.

Uwaga: Przetwarzanie danych osobowych poprzez Internet w systemie teleinformatycznym Urzędu będzie możliwe po zainstalowaniu w tym systemie odpowiednich zabezpieczeń zapewniających ochronę danych osobowych.

8. **Procedury wykonywania przeglądów i konserwacji systemu oraz nośników informacji służących do przetwarzania danych.**

§ 23

Przeglądy i konserwacje urządzeń systemu informatycznego Urzędu dokonywane są zgodnie z instrukcją ich użytkowania przez osobę posiadającą odpowiednie uprawnienia i pod nadzorem Administratora Bezpieczeństwa Informacji. Wskazane jest dokonywanie przeglądów nie rzadziej niż raz na miesiąc.

§ 24

Urządzenia i nośniki informacji służące do przetwarzania danych osobowych – przeznaczone do:

a) **likwidacji**: pozbawia się wcześniej zapisu tych danych - a w przypadku, gdy nie jest to możliwe – uszkadza się w sposób uniemożliwiający ich odczytanie;
b) **przekazania** innemu podmiotowi – nieuprawnionemu do otrzymania danych osobowych – pozbawia się wcześniej zapisu tych danych;
c) **naprawy:** pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych (ABI).

III. INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH.

§ 1

Użytkownik systemu informatycznego ma obowiązek zawiadomić Administratora Bezpieczeństwa Informacji lub inną upoważnioną przez niego osobę w przypadku naruszenia zabezpieczenia systemu polegającego na:

a) naruszeniu hasła dostępu (system nie reaguje na hasło lub je ignoruje – usunięty mechanizm hasła);
b) częściowym lub całkowitym braku bazy danych;
c) braku możliwości uruchomienia właściwej aplikacji (programu);
d) zmianie położenia urządzeń komputerowych;
e) kradzieży z pomieszczenia, w którym znajduje się sprzęt komputerowy.

§ 2

Użytkownik systemu informatycznego, w którym naruszono ochronę danych osobowych ma ponadto obowiązek:

a) powstrzymania się od wszelkich działań mogących utrudnić ustalenie sprawcy i okoliczności naruszenia zabezpieczenia danych osobowych oraz określenia szkód w systemie;
b) zabezpieczenia urządzeń komputerowych i pomieszczenia, w którym się one znajdują do czasu przybycia ABI lub osoby przez niego upoważnionej.

§ 3

Administrator Bezpieczeństwa Informacji po otrzymaniu zawiadomienia o naruszeniu zabezpieczeń ochrony danych osobowych w systemie informatycznym bezzwłocznie powinien:

a) powiadomić o tym administratora danych – Burmistrza;

b) podjąć działania uniemożliwiające dalsze nieuprawnione korzystanie z systemu – a w szczególności:
   - wymienić hasło użytkownika systemu;
   - zabezpieczyć przechowywane w urządzeniu dane osobowe;
   - dokonać analizy procedur korzystania z systemu;

c) przeprowadzić postępowanie wyjaśniające w celu ustalenia okoliczności i osoby odpowiedzialnej za naruszenie systemu ochrony oraz wielkości poczynionych szkód.

§ 4

W przypadku kradzieży z pomieszczenia, w którym znajduje się sprzęt komputerowy należy niezwłocznie powiadomić o zaistniałym fakcie policję.

ZESTAWIENIE ZAŁĄCZNIKÓW DO POLITYKI BEZPIECZEŃSTWA i INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM.

Załącznik Nr 1. – Oświadczenie (Wzór)

Załącznik Nr 2. – Upoważnienie (Wzór)

Załącznik Nr 3. – Wykaz pomieszczeń Urzędu, w których przetwarza się dane osobowe.

Załącznik Nr 4. – Wykaz zbiorów danych osobowych ze wskazaniem programów zastosowanych do przetwarzania tych danych.

Załącznik Nr 5.- Przepisy karne.

Załącznik Nr 1
do Polityki Bezpieczeństwa...

Zakroczym dnia .....

OŚWIADCZENIE

Ja, niżej podpisana .....

oświadczam,

że zostałam zapoznana z przepisami o ochronie danych osobowych zawartymi w:

1. ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101 poz. 926);

2. Rozporządzeniu ministra spraw wewnętrznych i administracji z dnia 29 kwietnia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;

3. Instrukcji ochrony danych osobowych Urzędu Gminy Zakroczym.

Znane są mi również przepisy o odpowiedzialności karnej za nieprzestrzeganie ochrony danych osobowych.

.....

(*data i podpis*)

Załącznik Nr 2
do Polityki Bezpieczeństwa...

Zakroczym dn. 26.04 2006r.

UPOWAŻNIENIE Nr 35/06

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101 poz. 926).

upoważniam:

Panią .....
zatrudnioną w .....
na stanowisku .....
do przetwarzania danych osobowych w zakresie wynikającym z obowiązków pracowniczych na zajmowanym stanowisku .

Pouczenie:

Osoba zatrudniona przy przetwarzaniu danych osobowych jest zobowiązana do zachowania ich w tajemnicy. Obowiązek ten istnieje również po ustaniu zatrudnienia. Niezachowanie tego obowiązku jest zagrożone odpowiedzialnością karną określoną w art. 49-54 ustawy wymienionej we wstępie upoważnienia.

Przyjęto do wiadomości i stosowania.

.....
(data i podpis pracownika)

.....
(administrator danych osobowych)

Załącznik Nr 3
Do Polityki Bezpieczeństwa...

WYKAZ POMIESZCZEŃ URZĘDU GMINY W KTÓRYCH PRZETWARZA SIĘ DANE OSOBOWE

L.p.	Nr pomieszczenia	Komórka organizacyjna	Osoba odpowiedzialna	Uwagi
1	2	3	4	5
		PARTER		
1	1	Referat Geodezji Gospodarki Przestrzennej i Inwestycji	Jarosław Furtak	
2	3	Kadry	Mirosława Milewska	Nie podlega rejestracji
3	5	Ewidencja Ludności	Agata Kostrzewska	
4	6	USC	Anna Fronczak	
		I PIĘTRO		
5	108	Referat Oświaty Kultury i Sportu	Kazimierz Szczerbatko	Nie podlega rejestracji
6	109		Jolanta Składanowska	
7	110	Podatki	Jolanta Majewska	
8	111	Ewidencja Działalności Gospodarczej	Elżbieta Zbonikowska	
9	113	Gospodarka Komunalna I Ochrona Środowiska	Dominika Wyzińska	
10	116	Referat Finansów i Budżetu	Elżbieta Nagel	
		GOPS ul o. H. Koźmińskiego 15		
11		Gminny ośrodek Pomocy Społecznej	Anna Lewicka	
		INNE		

Załącznik Nr 4
do Polityki Bezpieczeństwa...

WYKAZ ZBIORÓW DANYCH OSOBOWYCH URZĘDU GMINY.

Lp	Nazwa zbioru	Referat / stanowisko pracy	Zastosowany program	Uwagi
1	2	3	4	5
1	Ewidencja wydanych praw jazdy.	Ref. komunikacji - likwidacja 1.01.2000		Zaprzestano przetw. 1.01.2000
2	Księgowość i zobowiązania pieniężne	Referat finansów i budżetu		
3	Rejestry wydanych zezwoleń na budowę, na rozbiórkę, pozwoleń na użytkowanie...	Ref. Geodezji, Gosp. Przestrz. i Inwestycji		
4	Ewidencja Gruntów i Budynków jednostki ewidencyjnej Zakroczym.	Ref. Geodezji, Gosp.Przestrz. i Inwestycji		
5	Ewidencja Ludności i Dowody Osobiste	Ewidencja Ludności		
6	Ewidencja Podopiecznych Ośrodka Pomocy Społecznej	Gminny Ośrodek Pomocy Społecznej		
7	Urząd Stanu Cywilnego w Zakroczmiu	Urząd Stanu Cywilnego		
8	Dodatki Mieszkaniowe	Ref. Gospodarki Komunalnej i Ochrony Środowiska		
9				
10				
11				
12				
13				
14				

Załącznik Nr 5
Do Polityki Bezpieczeństwa...

PRZEPISY KARNE
(Wypis z Ustawy)

Art. 49.1. Kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do 2 lat.

2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.

Art. 50. Kto administrując zbiorem danych przechowuje w zbiorze dane osobowe niezgodnie z celem utworzenia zbioru, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 51. 1. Kto administrując zbiorem danych, lub będąc obowiązany do ochrony danych osobowych udostępnia lub umożliwia dostęp do nich osobom nieuprawnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

2. Jeżeli sprawca działa nieumyślnie podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 52. Kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 53. Kto do tego obowiązany nie zgłasza do rejestracji zbioru danych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 54. Kto administrując zbiorem danych nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w niniejszej ustawie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.