Z A R Z Ą D Z E N I E Nr 0151/ 7 /06

WÓJTA GMINY MAŁDYTY

z dnia 07 marca 2006 r.

w sprawie wdrożenia do stosowania w Urzędzie Gminy Małdyty „Polityki bezpieczeństwa" i „Instrukcji zarządzania systemem informatycznym"

Na podstawie art. 30 ust.1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2001 r. Nr 142, poz.1591 z późn. zmianami) oraz w związku z postanowieniami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz.926 z późn. zmianami) i rozporządzenia MSWiA 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. Nr 100, poz.1024), **zarządzam**:

§ 1. Wprowadzić następujące dokumenty :
1) „ Politykę bezpieczeństwa Urzędu Gminy Małdyty" stanowiącą załącznik nr 1
2) „ Instrukcję zarządzania systemem informatycznym „ stanowiącą załącznik nr 2
do przestrzegania i stosowania przez pracowników Urzędu Gminy Małdyty.

§ 2. Harmonogram wdrożenia stanowi załącznik nr 3 .

§ 3. Wykonanie zarządzenia powierzam Sekretarzowi Gminy.

§ 4. Zarządzenie wchodzi w życie z dniem 08 marca 2006 r.

WÓJT
mgr Antoni Smolak

Załącznik Nr 1 do zarządzenia
Nr 0151/ 7 /06 z dnia 7.03.2006r.
Wójta Gminy Małdyty

POLITYKA

BEZPIECZEŃSTWA

URZĘDU GMINY MAŁDYTY

Podstawa prawna:§ 3 i § 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2005 roku 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)

„Polityka bezpieczeństwa" to zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych wewnątrz Urzędu.
Zgodnie z art.36 ust. 2 oraz art. 39 a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych zwanej dalej ustawą, polityka bezpieczeństwa, powinna odnosić się całościowo do problemu zabezpieczenia danych osobowych zarówno do danych przetwarzanych tradycyjne jak i danych przetwarzanych w systemach informatycznych.

Celem polityki bezpieczeństwa jest wskazanie działań, jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie wykonać obowiązki administratora danych w zakresie zabezpieczenia danych osobowych.

§ 1. 1. Polityka bezpieczeństwa określa:

1) wykaz budynków i pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe,
2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych tych danych,
3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nim,
4) sposób przepływu danych pomiędzy poszczególnymi systemami,
5) środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

2. Polityka bezpieczeństwa dotyczy zabezpieczania danych osobowych przetwarzanych w Urzędzie Gminy Małdyty tradycyjnie i w systemach informatycznych.

§ 2. Ilekroć w polityce bezpieczeństwa jest mowa o:

1) **danych osobowych** – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,

2) **zbiorze danych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów,
3) **wykazie zbiorów danych osobowych** – rozumie się przez to wykaz zarejestrowanych, oraz nie podlegających rejestracji zbiorów danych osobowych,
4) **przetwarzaniu danych** – rozumie się przez 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,
5) **systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
6) **poufności danych** – rozumie się przez to właściwość zapewniającą, że dane się są udostępniane nieupoważnionym podmiotom,
7) **integralności danych** – rozumie się przez to właściwość zapewniającą, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
8) **rozliczalności** – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane tylko temu podmiotowi,
9) **administratorze bezpieczeństwa informacji** – rozumie się przez to pełnomocnika ds. ochrony informacji niejawnych,
10) **administratorze systemu** – rozumie się przez to osobę lub osoby upoważnione przez administratora danych osobowych do administrowania i zarządzania systemie informatycznym na terenie Urzędu Gminy Małdyty.

§ 3. 1. Obszar, w którym przetwarzane są dane osobowe tworzy budynek Urzędu Gminy Małdyty przy ulicy Kopernika 10.

2. Dane osobowe przetwarzane są metodą informatyczną i tradycyjną.

3.Szczegółowy wykaz pomieszczeń, w których przetwarzane są dane osobowe prowadzi administrator bezpieczeństwa informacji. Administrator bezpieczeństwa informacji posiada ewidencję programów, z których korzystają poszczególni pracownicy Urzędu Gminy.

4. W zakresie, o którym mowa w ust. 3 administrator systemu współpracuje z administratorem bezpieczeństwa informacji.

5. Kierownicy referatów oraz samodzielne stanowiska zobowiązani są do zgłaszania zmian oraz dokonywania aktualizacji obszaru, w którym przetwarzane są dane osobowe administratorowi bezpieczeństwa informacji.

§ 4.1. Pracownicy przetwarzający dane osobowe obowiązani są do prawidłowego ich zabezpieczenia na swoich stanowiskach pracy.

§ 5.1. Ochronę fizyczną obiektu (obszaru) stanowią zamki (kłódki) drzwiowe, okratowanie okien oraz system alarmowy.

2. Okratowaniu podlegają wszystkie otwory okienne w pomieszczeniach parterowych oraz przyziemiach piwnic a także otwór okienny na piętrze pokój nr 10. Drzwiami wejściowymi do budynku są 1) drzwi wejściowe główne (od strony ulicy Kopernika), 2) drzwi wejściowe boczne (od strony podwórza).

3.Jeden zestaw kluczy do pomieszczeń służbowych posiada sprzątaczka , która otwiera drzwi do pomieszczeń przed rozpoczęciem pracy i zamyka po zakończeniu pracy Urzędu. Po jednym kluczu do drzwi pomieszczenia posiada pracownik (bądź jeden z pracowników) pracujący w danym pomieszczeniu. Komplet kluczy zapasowych do pomieszczeń znajduje się w szafie metalowej w pokoju nr 10.

4. Pomieszczenia służbowe winny być zamknięte każdorazowo pod nieobecność osób w nich pracujących.

§ 6. 1. Pracownikom wolno przebywać na terenie Urzędu tylko w godzinach ich pracy, a po godzinach pracy oraz w dni wolne od pracy tylko po uzyskaniu zezwolenia od Wójta Gminy a w razie jego nieobecności Sekretarza Gminy.

2. Osoba przebywająca na terenie Urzędu poza godzinami pracy oraz w dni wolne od pracy obowiązana jest każdorazowo:
- dokonać zarejestrowania przyjścia zgodnie z godziną przyjścia,
- dokonać zarejestrowania wyjścia, zgodnie z godziną wyjścia w wyłożonej liście obecności.

3. Zakaz przebywania na terenie Urzędu poza godzinami pracy i w dni wolne od pracy nie dotyczy: sekretarza gminy, skarbnika gminy, kierownika i zastępcy kierownika USC, pełnomocnika ds. ochrony informacji niejawnych.

§ 7. Wszelkie nieprawidłowości w zakresie, o którym mowa w § 5 i 6 należy niezwłocznie zgłaszać do Referatu Organizacyjnego i Spraw Obywatelskich oraz administratora bezpieczeństwa informacji.

§ 8. 1. Do zdarzeń naruszających ochronę danych osobowych należą:

1) **zagrożenia losowe zewnętrzne** (np. klęski żywiołowe, przerwy 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 osobowych.
2) **zagrożenia losowe wewnętrzne** (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych,
3) **zagrożenia zamierzone, świadome i celowe** – najpoważniejsze zagrożenia, naruszenia poufności danych,(zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenie te możemy podzielić na: 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. 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 papierze(wydrukach), dyskietkach w formie niezabezpieczonej.

§ 9. 1. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych w zbiorach, prowadzonych w Urzędzie Gminy Małdyty, stanowi **załącznik nr 1** do polityki bezpieczeństwa.

2. Kierownicy referatów oraz samodzielne stanowiska niezwłocznie zgłaszają administratorowi bezpieczeństwa informacji wszelkie zmiany w zbiorach danych osobowych oraz nowe zbiory danych osobowych, które podlegają zgłoszeniu Generalnemu Inspektorowi Ochrony Danych Osobowych.

§ 10. 1. Opisu struktury zbioru danych wskazujących zawartość poszczególnych pól informacyjnych i powiązań miedzy nimi dokonuje administrator bezpieczeństwa informacji.

2. Opisu, o którym mowa w ust. 1 , w odniesieniu do zbiorów danych przetwarzanych w systemach informatycznych dokonuje administrator systemu.

§ 11. 1. Administratorem danych osobowych zawartych i przetwarzanych w systemach informatycznych i metodą tradycyjną Urzędu Gminy Małdyty jest Wójt.

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

1) zabezpieczyć dane przed ich udostępnianiem osobom nieupoważnionym,
2) zapobiegać przed zabraniem danych przez osobę nieuprawnioną,
3)zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.

3. Do zastosowanych środków technicznych należy:

1) przetwarzania danych osobowych w wydzielonych pomieszczeniach położonych w strefie administracyjnej,
2) zabezpieczenia wejścia do pomieszczeń, o których mowa w pkt. 1,
3) wyposażenie pomieszczeń w zamki, itp. narzędzia i urządzenia dające gwarancję bezpieczeństwa dokumentacji.

4. Do zastosowanych środków organizacyjnych należą przede wszystkim następujące zasady:

1) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy przetwarzaniu danych osobowych,
2) przeszkolenie osób, o których mowa w pkt. 1, w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych,
3) kontrolowanie otwierania i zamykania pomieszczeń, w których są przetwarzane dane osobowe,

5. Środkami niezbędnymi do zapewnienia poufności , integralności i rozliczalności przetwarzanych danych osobowych w systemach informatycznych w Urzędzie Gminy Małdyty są:
1)system nadawania haseł i identyfikatorów użytkownikom,
2)stosowanie ochrony antywirusowej.

6. Sposób przepływu danych pomiędzy poszczególnymi systemami informatycznymi w sieci lokalnej w Urzędzie Gminy Małdyty, określa **załącznik nr 2** do polityki bezpieczeństwa.

§ 12. Przetwarzanie danych osobowych w zbiorach prowadzonych w systemach informatycznych jest dopuszczalne wyłącznie przez osoby posiadające upoważnienie wydane przez Wójta Gminy Małdyty. Wzór upoważnienia stanowi **załącznik nr 3** do Polityki bezpieczeństwa.

§ 13. Osoby przetwarzające dane osobowe w sposób tradycyjny przetwarzają je na podstawie uprawnień wynikających z indywidualnych zakresów czynności.

§ 14. Dane osobowe w wersji papierowej a także wydruki i kopie, należy niszczyć w niszczarce. Zabronione jest usuwanie danych przez wyrzucenie ich do kosza na odpadki.

§15. Kierownicy referatów zapewniają przestrzeganie polityki bezpieczeństwa w pracy referatu.

§ 16.1. Administrator danych Wójt lub osoba przez niego wyznaczona, którą jest „Administrator Bezpieczeństwa Informacji" sprawuje nadzór Nd p[przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.

2. Administrator Bezpieczeństwa sporządza roczne sprawozdanie i przedstawia Wójtowi Gminy.

§ 17. 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.

§ **18** . Administrator Bezpieczeństwa zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych wg wzoru stanowiącego **załącznik nr 4** do niniejszego dokumentu.

§ **19**.Z uwagi na fakt coraz powszechniejszego wykorzystywania Internetu na naszych stanowiskach pracy(zwłaszcza niebezpieczne w dzisiejszych czasach, powszechne usługi www i e-mail) oprócz szerokiej i szybkiej dostępności do informacji niosą za sobą wiele zagrożeń związanych z podsłuchem elektronicznym, wirusami, zdalną kontrolą itp. należy tym tematom poświęcić w najbliższym czasie więcej uwagi. Konstruując budżet gminy należy bezwzględnie planować środki również na ten cel. Niektóre działania zostały już podjęte ale jest jeszcze wiele do zrobienia.
Należy również zauważyć , że polityka bezpieczeństwa to nie tylko samo oprogramowanie, to również świadomość i odpowiedzialność pracowników-użytkowników Internetu, którą podnieść można tylko poprzez właściwe szkolenia i wdrażanie odpowiednich instrukcji i regulaminów (takie działania są w naszym Urzędzie podejmowane i nie wymagają one nakładów finansowych) ale są niezbędne i powinny iść w parze z wydatkami na odpowiednie oprogramowanie i urządzenia zabezpieczające.

WÓJT
mgr Antoni Smolak

Załącznik nr 1 do Polityki
Bezpieczeństwa wprowadzonej
zarządzeniem Nr 0151/7/06
z dnia 7marca 2006 r.

WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA DANYCH W ZBIORACH PROWADZONYCH W URZĘDZIE GMINY MAŁDYTY

WÓJT
mgr Antoni Smolak

Załącznik nr 2 do Polityki Bezpieczeństwa
wprowadzonej zarządzeniem nr0151-7/06.
Wójta Gminy Małdyty z dnia7.03.2006r.

SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI INFORMATYCZNYMI W SIECI LOKALNEJ URZĘDU GMINY MAŁDYTY

WÓJT
inż. Antoni Smolak

35

Załącznik Nr 3
do Polityki Bezpieczeństwa

Małdyty, dnia.....2006 r.

UPOWAŻNIENIE

Na podstawie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, późn. zmianami) Administrator Danych Osobowych Urzędu Gminy Małdyty mgr Antoni Smolak

upoważnia Pana/Panią .....
Nr identyfikatora.....

do przetwarzania danych osobowych, dotyczących .....

.....

Administrator Danych zobowiązuje Pana / Panią do zachowania w tajemnicy przetwarzane dane osobowe oraz sposoby ich zabezpieczenia.

.....
podpis

Oświadczam, że przyjęłam do realizacji dokumenty „ Politykę Bezpieczeństwa" i „Instrukcję Zarządzania Systemem Informatycznym". Ponadto zobowiązuję się do zachowania w tajemnicy przetwarzane dane osobowe oraz sposoby ich zabezpieczania.

WÓJT
mgr Antoni Smolak

.....
podpis

Załącznik Nr 4 do
Polityki Bezpieczeństwa

EWIDENCJA

Osób, które zapoznały się z dokumentem „Polityka Bezpieczeństwa" i zobowiązały się do stosowania zasad w nim zawartych

L.p.	Nazwisko i imię	Stanowisko służbowe	Data	Własnoręczny podpis

WÓJT
mgr Antoni Smolak

41

Załącznik Nr 2
do zarządzenia nr 0151/ 7./06
z dnia 7.marca 2006 r.
Wójta Gminy Małdyty

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE GMINY MAŁDYTY

Podstawa prawna:

- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz.926 z późn. zmianami).
- Rozporządzenie MSWiA 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. Nr 100, poz. 1024).

Administrator danych osobowych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

W celu zrealizowania tych obowiązków administrator danych wprowadza instrukcję zarządzania systemem informatycznym jako dokument obowiązujący na terenie Urzędu Gminy Małdyty.

Administrator danych zobowiązuje podwładnych do przestrzegania postanowień tej instrukcji.

1. Przez administratora bezpieczeństwa informacji należy rozumieć osobę lub osoby upoważnione przez administratora danych osobowych do administrowania i zarządzania systemami informatycznymi na terenie Urzędu Gminy Małdyty. W Urzędzie Gminy Małdyty administratorem bezpieczeństwa informacji jest osoba pracująca jako pełnomocnik d.s ochrony informacji niejawnych. Wójt Gminy(administrator danych osobowych wyznacza również osobę upoważniona do zastępowania administratora bezpieczeństwa informacji.

2. Administrator Bezpieczeństwa Informacji realizuje zadania w zakresie ochrony danych, a w szczególności:

1) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Urzędu,

2) podejmowania stosownych działań zgodnie z „ Polityką bezpieczeństwa" w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym,

3) niezwłocznego informowania Administratora danych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,

4) nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych.

3. Osoba zastępująca Administratora Bezpieczeństwa Informacji powyższe zadania realizuje w przypadku nieobecności Administratora Bezpieczeństwa Informacji.

4. Osoba zastępująca składa Administratorowi Bezpieczeństwa Informacji relację z podejmowanych działań w czasie jego nieobecności.

5. Przetwarzanie danych osobowych to wykonywanie na nich operacji takich jak: zbieranie, utrwalanie, przechowywanie , opracowywanie , zmienianie, udostępnianie, usuwanie zarówno w systemie informatycznym jak i ręcznym .

6. Dane osobowe z użyciem stacjonarnego sprzętu komputerowego są przetwarzane w Urzędzie Gminy Małdyty w obszarach:

- parter 9 pokoje nr : 1,2,3,4,5,6,7)
- piętro (pokoje nr: 9,10,11,12, 14,15).

7. Przebywanie w pomieszczeniach znajdujących się wewnątrz obszaru, o którym mowa w pkt. 3 osób nieuprawnionych do dostępu do danych osobowych jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych.

8. Pomieszczenia, w których przetwarzane są dane osobowe powinny być zamykane na czas nieobecności w nich osób zatrudnionych w sposób uniemożliwiający dostęp do nich osób trzecich.

9. Procedura rozpoczęcia i zakończenia pracy:

1) na stanowiskach, na których przetwarzane są dane osobowe ekrany monitorów powinny być tak ustawione, aby osoby nieupoważnione nie miały dostępu do informacji na nich wyświetlanych,

2) bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu właściwego identyfikatora i hasła,

- każdy z użytkowników korzystając z systemów przetwarzających dane osobowe powinien posiadać swój identyfikator i hasło,
- hasła powinny być zmieniane raz w miesiącu i składać się z co najmniej 6 znaków (najlepiej liter i cyfr),
- hasło nie może być zapisywane w miejscu dostępnym dla osób nieuprawnionych. Użytkownik nie może udostępniać hasła i stanowiska roboczego osobom nieuprawnionym.

3)użytkownik powinien upewnić się, że osoby nie upoważnione nie mają możliwości wglądu do danych,

4) w razie przerwania pracy należy zastosować wygaszacz ekranu,

5) użytkownik powinien upewnić się czy dane zostały zarejestrowane , aby uniknąć utraty danych z powodu awarii,

6) podczas nieobecności osób zatrudnionych przy informatycznym przetwarzaniu danych osobowych pomieszczenia, w których przetwarzane są dane , nie mogą być udostępniane osobom postronnym,

7) zakończenie pracy związanej z przetwarzaniem danych powinno odpowiadać wszystkim regułom bezpieczeństwa informacji.

10. Rejestr użytkowników systemów informatycznych prowadzi administrator systemu.
W rejestrze użytkowników znajdują się następujące dane:
- nazwisko i imię
- identyfikator
- stanowisko
- referat, w którym użytkownik jest zatrudniony
- wskazanie zbiorów, do których użytkownik jest uprawniony
- zakres uprawnień do systemów

W przypadku wyrejestrowania użytkownika jego identyfikator nie może być przekazany innemu pracownikowi.

11. Zabrania się użytkownikom systemu informatycznego:
1) udostępniania stanowisk roboczych oraz istniejących w nich danych (w postaci pisemnej lub elektronicznej) osobom nieupoważnionym ,
2) wykorzystywanie sieci komputerowej w celach innych niż wyznaczone przez administratora danych osobowych,
3) samowolnego instalowania i użytkowania programów komputerowych (posiadających licencji),
4) trwałego lub okresowego kopiowania programów w całości lub części bez zgody administratora systemu,
5) publicznego rozpowszechniania programów komputerowych przez możliwość dostępu do sieci wewnętrznej lub Internetu,
6) przenoszenia programów komputerowych z własnego stanowiska roboczego na inne stanowisko,
7) udostępniania osobom postronnym programów komputerowych przez możliwość dostępu do sieci wewnętrznej lub internetu,
8) używania nośników udostępnianych przez osoby postronne i podejrzanych o „zainfekowanie wirusem" : w razie podejrzenia o „zainfekowanie wirusem nośnika danych (dyskietki lub dysku twardego) użytkownik ma obowiązek niezwłocznie poinformować o tym administratora danych osobowych lub inną uprawnioną osobę,
9) używania oprogramowania w większym zakresie niż pozwala na to umowa licencyjna.

12. Zobowiązuje się kierowników referatów oraz samodzielne stanowiska do informowania administratora bezpieczeństwa informacji o każdorazowej ingerencji „firm trzecich" w strukturę systemu informatycznego Urzędu Gminy Małdyty, dostarczenia umów licencyjnych oprogramowań oraz poświadczeń bezpieczeństwa informacji w.w firm.

13. Czas pracy przy urządzeniach informatycznych jest tożsamy z godzinami pracy Urzędu, wynikającymi z Regulaminu Organizacyjnego Urzędu Gminy Małdyty.

14. Na pracę na urządzeniach informatycznych poza godzinami pracy konieczna jest zgoda administratora systemu.

15. Archiwizowanie danych :
1) kopie awaryjne wykonuje się codziennie na płytach CD-R lub na oddzielnym twardym dysku . Te nośniki danych, przechowuje się w specjalnie zamykanej szafie , do której dostęp mają tylko osoby uprawnione.
2) kopie przechowuje się przez okres 12 miesięcy. Kopii awaryjnych nie potrzeba wykonywać, jeżeli w danym dniu nie dokonano zapisu zmieniającego bazę danych.
3) likwidacja nośników zawierających kopie zapasowe danych polega na ich uszkodzeniu uniemożliwiającym odzyskanie.

16.Systemy komputerowe, programy i nośniki są sprawdzane na obecność „wirusów" komputerowych z częstotliwością wyznaczoną przez administratora. Aby uniknąć infekcji „ wirusów" komputerowych użytkownicy korzystający z internetu nie powinni odwiedzać stron internetowych o podejrzanej tematyce (np. stron hakerskich czy erotycznych).

17. Przeglądy i konserwacje systemu i zbiorów danych wykonuje się w razie potrzeby, lecz nie rzadziej niż jeden raz w miesiącu.

18. Komunikacja w sieci komputerowej służy wyłącznie do przesyłania danych oraz informacji pomiędzy użytkownikami w sprawach funkcjonowania Urzędu.

19.Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych pozbawia się wcześniej zapisu danych. Dotyczy to także urządzeń przeznaczonych do naprawy chyba, że naprawa odbędzie się pod nadzorem osoby upoważnionej przez administratora danych.

20. Administrator danych osobowych ustali osobę lub osoby odpowiedzialne za ustalanie potrzeb w zakresie komputeryzacji Urzędu (uwzględniając plany budżetowe w tym zakresie), zakup sprzętu komputerowego oraz oprogramowania .

Sporządziła.
Stanisława Domańska

WÓJT
mgr Antoni Smolak

Załącznik Nr 3
do zarządzenia Wójta Gminy Małdyty
Nr 0151-7 /06 z dnia 7 marca 2006 r.

HARMONOGRAM

wdrożeniowy realizacji zarządzenia Wójta Gminy Małdyty Nr 0151- 7/06 z dnia 7 marca 2006 r.

l.p.	Zadanie	Termin wykonania	Realizator	Uwagi:
1.	**W zakresie legalności**: 1) założenie ewidencji komputerów, zainstalowanych programów, 2) ustalenie odpowiedzialności prawnej pracowników za powierzony sprzęt i oprogramowanie, 3) ustalenie, kto odpowiada za zakup sprzętu komputerowego, i oprogramowania , określenie kosztów, i potrzeb w tym zakresie, 4) powołanie administratora bezpieczeństwa informacji, 5) powołanie zarządzającego oprogramowaniem,	30.04.06 30.03.06 15.04.06 30.03.06 15.04.06	Administrator sieci i zbiorów informatycznych Administrator danych osobowych „ „ ABI	
2.	**W zakresie ochrony komputera**:		Administrator	

	1) powołanie administratora sieci i zbiorów informatycznych, 2) zabezpieczenie dostępu do Internetu do stron o podejrzanej tematyce, 3) zabezpieczenie komputerów przed „wirusami" 4) ewidencja identyfikatorów i haseł,	30.04.06 30.05.06 30.05.06	bezpieczeństwa informacji Administrator Sieci i zbiorów informatycznych " ABI	
3.	**W zakresie ochrony danych osobowych:** 1)) dokonanie analizy potrzeb w sprawie wydania poświadczeń bezpieczeństwa dla pracowników 2) założenie ewidencji wydanych poświadczeń bezpieczeństwa , 3) dokonanie przeglądu gdzie przechowywane są dokumenty i czy są one przechowywane prawidłowo, jeżeli nie to doprowadzić do prawidłowego ich przechowywania, 4)założenie ewidencji zgłoszonych do GIODO zbiorów danych, 5) dokonanie analizy zbiorów danych pod kątem potrzeby ich zgłoszenia do rejestracji przez GIODO. 6) dokonać sprawdzenia zabezpieczenia danych osobowych podczas ich przetwarzania : - „czyste biurko", - kto widzi monitor, - kontrola dostępu do danych biurko, szafy, pomieszczenia,	30.05.06 30.05.06 15.06.06 30.05.06 30.05.06 30.06.06	ABI ABI ABI ABI ABI ABI i Administrator sieci i zbiorów informatycznych	
4.	**W zakresie ochrony fizycznej**: 1) dokonanie analizy czy istniejące monitorowanie Urzędu jest wystarczające, jeżeli nie to określić inny sposób monitorowania oraz koszt i termin realizacji, 2)dokonanie analizy zabezpieczenia fizycznego budynku, pomieszczeń, szaf i biurek (zamki , kłódki) , 3) przygotowanie i wdrożenie instrukcji p.przeciwpożarowej	30.06.06 30.06.06 30.06.06	ABI i kier. Ref.GKM ABI ABI	
5	**W zakresie zabezpieczenia organizacyjnego realizacji polityki**			

	bezpieczeństwa i i innych dokumentów związanych z realizacja ochrony danych osobowych, 1) szkolenie kierowników referatów i samodzielnych stanowisk w zakresie zapoznania się z polityką bezpieczeństwa oraz instrukcją zarządzania systemem informatycznym, 2) szkolenie wszystkich pracowników z zakresu ochrony komputera	3 razy w okresie od 01.05 do 30.09.06 30.06.06	ABI Administrator sieci i zbiorów informatycznych
6.	Sprawdzenie w praktyce realizacji postanowień polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym….. przez poszczególnych pracowników Urzędu Gminy.	30.12.06	ABI

Sporządziła.
Stanisława Domańska

WÓJT
mgr Antoni Szkolak