Załącznik nr 1 do zarządzenia nr 316/06
BMiG Małogoszcz z dnia 31 lipca 2006r.

POLITYKA BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH W URZĘDZIE MIASTA I GMINY MAŁOGOSZCZ

Rozdział I

Zasady ogólne

§ l

Polityka bezpieczeństwa została opracowana na podstawie ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 r. nr 101, poz.926 z późn.zm.) w celu realizacji rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 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. z 2004 r. nr 100, poz. 1024).

§ 2

Przez użyte w polityce bezpieczeństwa następujące określenia należy rozumieć:

1) **dane osobowe** — każda informacja dotycząca osoby fizycznej, pozwalająca na określenie tożsamości tej osoby,
2) **zbiór danych osobowych** — każdy posiadający strukturę zestaw danych o charakterze osobowym dostępny według określonych kryteriów,
3) **przetwarzanie danych** — 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,
4) **Administrator Danych Osobowych** — Burmistrz Miasta i Gminy Małogoszcz,
5) **Administrator Bezpieczeństwa Informacji** — osoba wyznaczona przez administratora danych osobowych odpowiedzialna za bezpieczeństwo danych osobowych,
6) **Urząd** — Urząd Miasta i Gminy Małogoszcz
7) **pracownik samorządowy** — osoba zatrudniona w ramach stosunku pracy w Urzędzie,
8) **użytkownik** — osoba przetwarzająca dane,

9) **system informatyczny** — zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych stosowanych w celu przetwarzania danych.

Rozdział II

Cele i zasady bezpieczeństwa zbiorów danych osobowych

§ 3

1. Przez politykę bezpieczeństwa rozumie się zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych w Urzędzie.
2. Celem polityki bezpieczeństwa jest zapewnienie kierunków działania i wsparcie administratora danych osobowych dla bezpieczeństwa danych.
3. Celem przetwarzania danych osobowych zawartych w zbiorach danych osobowych w Urzędzie jest realizacja przez pracowników zadań określonych przepisami prawa.
4. Cel, o którym mowa w ust.3 osiąga się przez zachowanie szczegółowej staranności w realizacji przedsięwzięć dotyczących ochrony interesów osób, których dane dotyczą, a w szczególności przetwarzanie danych zgodnie z:
   a) obowiązującymi w tym zakresie przepisami,
   b) zasadami udostępniania danych osobowych - zgodnie z załącznikiem nr 1,
   c) określonym okresem przechowywania danych identyfikujących osobę fizyczną,
   d) obowiązującymi procedurami ochrony danych osobowych.

Rozdział III

Ogólne zasady bezpieczeństwa zbiorów

§ 4

1. Naczelną zasadą bezpieczeństwa zbiorów danych osobowych obowiązującą pracowników Urzędu jest zachowanie tajemnicy o zasadach przetwarzania danych osobowych podczas wykonywania obowiązków służbowych.
2. Możliwość wystąpienia zagrożeń bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym lub w zbiorach gromadzonych w tradycyjnych rejestrach i kartotekach nakłada na użytkowników obowiązek stosowania zabezpieczeń organizacyjnych i technicznych zbiorów polegających głównie na:

a) zastosowaniu odpowiednich środków technicznych i organizacyjnych w celu zapewnienia ochrony danych osobowych oraz unowocześnianiu ich wraz z rozwojem nauki i techniki informatycznej,
b) wykorzystanie takiej ochrony danych osobowych, która zabezpiecza zbiory przed uszkodzeniem, modyfikacją, ujawnieniem lub zniszczeniem,
c) ochronie danych przed wglądem osób nieupoważnionych,
d) zabezpieczeniu komputerów przenośnych przetwarzających dane osobowe,
e) stosowaniu nadzoru i kontroli w zakresie odnotowywania wszelkich zmian danych osobowych w zbiorach,
f) udostępnianiu danych tylko instytucjom do tego uprawnionym oraz osobom fizycznym, zgodnie z obowiązującymi przepisami prawa.

3. Zachowanie bezpieczeństwa zbiorów danych osobowych wymaga, aby przesyłanie danych osobowych za pomocą faksu, urządzeń teletransmisji lub Internetu odbyło się w sytuacjach wykorzystania odpowiednich urządzeń zabezpieczających przekaz oraz po uzyskaniu pisemnej zgody od administratora lub osoby uprawnionej.
4. Zasadą bezpieczeństwa zbiorów danych osobowych jest przetwarzanie danych przez użytkowników zgodnie z obowiązującymi procedurami ochrony.

§ 5

Użytkownicy przetwarzający dane osobowe powinni posiadać stosowne uprawnienia oraz złożyć zobowiązanie do przestrzegania określonych zasad bezpieczeństwa zbiorów, a w szczególności:
a) posiadać imienne upoważnienie do przetwarzania danych osobowych i o dostępie do systemu informatycznego w którym przetwarzane są dane osobowe, wydane przez administratora,
b) posiadać w zakresie obowiązków zobowiązanie dotyczące indywidualnej odpowiedzialności za przestrzeganie przepisów o ochronie danych osobowych,
c) złożyć zobowiązanie o zachowaniu w tajemnicy zasad bezpieczeństwa danych osobowych stosowanych w czasie ich przetwarzania nawet po ustaniu stosunku pracy,
d) zapoznać się z aktualnymi przepisami dotyczącymi ochrony danych osobowych.

Rozdział IV

Wykaz budynków, pomieszczeń lub części pomieszczeń w których przetwarzane są dane osobowe

§ 6

1. Zasadą bezpieczeństwa zbiorów danych osobowych jest określenie budynków i pomieszczeń lub części pomieszczeń tworzących obszary, w których przetwarzane są dane osobowe z użyciem sprzętu komputerowego.
2. W obszarach, w których przetwarzane są dane osobowe, przebywanie osób nieupoważnionych jest ograniczone i odbywać się może tylko w obecności użytkowników i za zgodą administratora.
5. Obszar do przetwarzania danych osobowych obejmuje:
   a) miejsca, w których wykonuje się operacje na danych osobowych,
   b) miejsca gdzie przechowuje się nośniki informacji zawierające dane osobowe:
   - szafy z dokumentacją papierową
   - szafy zawierające komputerowe nośniki informacji z kopiami zapasowymi danych,
   - serwery,
   - stacje komputerowe,
   - macierze dyskowe, na których dane osobowe są przetwarzane na bieżąco,
   - sprzęt aktywny sieci,
   - okablowanie sieciowe,
   c) miejsca, gdzie gromadzone są uszkodzone komputerowe nośniki danych:
   - taśmy,
   - dyski,
   - płyty CD,
   - uszkodzone komputery,
   - inne urządzenia z nośnikami obejmujące dane osobowe,
   d) archiwum.

   Wykaz obszarów do przetwarzania danych osobowych prowadzi administrator bezpieczeństwa informacji według wzoru stanowiącego załącznik nr 2.
6. Osoby wchodzące do obszaru i wychodzące z niego są zobowiązane do zabezpieczenia wejścia poprzez zamknięcie drzwi.
7. Obszar pomieszczeń, w których przetwarza się dane osobowe jest zamknięty na czas nieobecności w nim osób upoważnionych. Ewidencję osób upoważnionych do pobierania kluczy od pomieszczeń przetwarzania danych osobowych prowadzi administrator bezpieczeństwa informacji według wzoru stanowiącego załącznik nr 3.
8. Przebywanie osób nieupoważnionych na terenie obszaru jest dozwolone tylko i wyłącznie w obecności osób zatrudnionych przy przetwarzaniu danych osobowych.

Rozdział V

Wykaz zbiorów danych osobowych.

§ 7

1 .Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych osobowych określającym nazwy i lokalizacje miejsc (pomieszczenia, nazwa komputera, nazwa macierzy dyskowej), w których znajdują się zbiory danych osobowych, przetwarzane na bieżąco oraz nazwy i lokalizacje programów (aplikacje, systemy zarządzania bazami danych , systemy operacyjne, oprogramowanie narzędziowe — na przykład do bezpiecznego usuwania danych) używanych do ich przetwarzania.
2. Administrator Bezpieczeństwa Informacji prowadzi wykaz zbiorów danych osobowych według wzoru określonego w załączniku nr 4 do instrukcji.
3.Administrator Bezpieczeństwa Informacji prowadzi ewidencję okresów oraz miejsc przechowywania zbiorów danych osobowych według załącznika nr 5.
4. Administrator Bezpieczeństwa Informacji prowadzi ewidencję oprogramowania według załącznika nr 6.

Rozdzial VI

Systemy ochrony

§ 8

Szkolenia

Administrator Bezpieczeństwa Informacji odpowiada za przeprowadzenie szkolenia pracowników obejmujących zapoznanie z obowiązującymi aktami prawnymi w zakresie ochrony danych osobowych i ustanowionymi w Urzędzie zasadami bezpiecznego ich przetwarzania. Uczestnictwo w szkoleniu jest warunkiem dopuszczenia pracowników do korzystania z systemów informatycznych przetwarzających dane osobowe.
Listę pracowników podlegających szkoleniu prowadzi się według załącznika Nr 7.

§ 9

Zarządzanie ryzykiem.

1. Administrator Bezpieczeństwa Informacji przeprowadza dokładną analizę zagrożeń i ryzyka związanych z przetwarzaniem danych osobowych, a w szczególności:
a) identyfikuje zagrożenia wpływające na bezpieczeństwo przetwarzanych danych osobowych,
b) analizuje wrażliwość systemu informatycznego na zagrożenia związane z bezpieczeństwem danych osobowych,
c) ocenia ryzyko związane z przetwarzaniem danych osobowych,
d) wdraża metody zabezpieczające dane osobowe, a minimalizujące zagrożenia,
e) analizuje ryzyko po zastosowaniu środków zabezpieczających.

§ 10

Poziomy bezpieczeństwa systemu

1. Uwzględniając zagrożenia Administrator Bezpieczeństwa Informacji wprowadza poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym.
2. Każdy z programów ma możliwość ustawienia trybu pracy.
3. Programy mogą pracować na następujących poziomach:
   - **brak**: ten poziom może być stosowany tylko wówczas, gdy program nie przetwarza danych osobowych, a jest wykorzystywany tylko dla celów szkoleniowych; przy pracy programów na tym poziomie nie jest kontrolowana minimalna długość hasła, ani czas jego zmiany,
   - **podstawowym**: ten poziom może być stosowany tylko wówczas, gdy w programie nie są przetwarzane dane o pochodzeniu rasowym lub etnicznym, o poglądach politycznych, przekonaniach religijnych i filozoficznych, przynależności partyjnej lub związkowej, o stanie zdrowia, kodzie genetycznym, nałogach, życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydawanych w postępowaniu sądowym lub administracyjnym Dodatkowym uwarunkowaniem umożliwiającym pracę na systemie podstawowym jest to, że żadne z urządzeń systemu informatycznego nie może być połączone z siecią publiczną. O tym czy dany program może pracować na poziomie podstawowym powinien zadecydować Administrator Danych Osobowych uwzględniając dane przetwarzane przez programy oraz architekturę systemu komputerowego. Jeżeli program pracuje na tym poziomie, to program kontroluje minimalną długość hasła (6 znaków) oraz częstotliwość jego zmian (nie rzadziej niż 30 dni),
   - **podwyższonym**: ten poziom może być stosowany tylko wówczas, gdy żadne z urządzeń systemu informatycznego nie może być połączone z siecią publiczną. Nie jest to zależne od rodzaju danych przetwarzanych przez program. O tym czy dany program może pracować na poziomie podwyższonym powinien zadecydować Administrator Danych Osobowych uwzględniając dane przetwarzane przez programy oraz architekturę systemu

komputerowego. Jeżeli program pracuje na tym poziomie, to program kontroluje minimalną długość hasła (8 znaków) oraz częstotliwość jego zmian (nie rzadziej niż 30 dni),

- **wysokim**: ten poziom musi być stosowany, jeśli choć jedno urządzenie systemu informatycznego podłączone jest do sieci publicznej. Z punktu widzenia programu nie ma różnicy w kontroli dostępu do programu oraz kontroli haseł pomiędzy poziomem podwyższonym a wysokim. Poziom wysoki zobowiązuje Administratora Danych Osobowych do wdrożenia dodatkowych logicznych lub fizycznych zabezpieczeń pomiędzy systemem informatycznym Administratora a siecią publiczną.

§ 11

Z technicznych aspektów zabezpieczeń zastosowanych w programach należy stosować:

a) kontrolę dostępu do programów komputerowych z użyciem identyfikatora i hasła,
b) blokadę możliwości ponownego użycia identyfikatora użytkownika, który utracił prawo do korzystania z niego.

§ 12

Należy zapewnić ochronę baz danych programów przetwarzających dane osobowe przed dostępem osób niepowołanych.

§ 13

W przypadku umieszczenia programów i danych na dysku lokalnym komputera nie podłączonego do sieci, należy ograniczyć dostęp do tego komputera poprzez ochronę pomieszczenia lub ochronę samego komputera. Ochrona komputera możliwa jest poprzez hasło (ustawione w BIOS), którego znajomość warunkuje uruchomienie komputera i wczytanie systemu operacyjnego. W przypadku nowych komputerów wyposażony w system operacyjny Windows 2000 lub Windows XP należy tak skonfigurować prawa dostępu, aby programy wraz z bazami danych znajdowały się w miejscu niedostępnym dla innych użytkowników tego komputera. Starsze systemy WINDOWS 95/98/Me nie posiadają takiej możliwości skonfigurowania zabezpieczeń, aby z jednego komputera mogło korzystać wiele osób i dane były odpowiednio zabezpieczone. Jeżeli do komputera dołączone są urządzenia we/wy umożliwiające instalację innych programów i ich wczytywanie z dyskietek lub CD to dodatkowo komputer powinien zostać zabezpieczony przez oprogramowanie antywirusowe, które zminimalizuje zagrożenie instalacji oprogramowania zagrażającego całemu komputerowi, a także bazom danych.

§ 14

W przypadku umieszczenia programów i danych na dysku sieciowym niezależnie od zabezpieczeń poszczególnych komputerów, należy zadbać o właściwy poziom zabezpieczenia sieci lokalnej. Sprowadza się to przede wszystkim do takiego zabezpieczenia katalogów z programami, aby były one niedostępne dla osób nieuprawnionych do korzystania z programów komputerowych przetwarzających dane osobowe. Inni użytkownicy sieci komputerowej nie powinni posiadać odczytu ani zapisu w katalogach z w/w programami komputerowymi.

§ l5

W przypadku podłączenia sieci lokalnej z siecią publiczną (Internet) należy obligatoryjnie zastosować fizyczne lub logiczne zabezpieczenia. Mogą to być zarówno zabezpieczenia o charakterze sprzętowym lub też programowym.

§l6

Administrator powinien bezwzględnie zadbać o uaktualnienie stosowanego oprogramowania systemowego tak, aby były zainstalowane wszystkie poprawki dostarczane przez ich producentów.

§ l7

Uwzględniając kategorie danych osobowych oraz stopień bezpieczeństwa ich przetwarzania w systemie informatycznym Urzędu wprowadza się poziom wysoki bezpieczeństwa systemu.

§18

1. Pracownicy biorący udział w procesie przetwarzania danych osobowych są odpowiedzialni za zabezpieczenie ich poufności, integralności i dostępności.
2. Pracownicy zobowiązani są do przestrzegania istniejących procedur i stosowania środków zabezpieczających dane osobowe — wdrożonych w Urzędzie.

§ l9

Zabezpieczenie przetwarzanych danych osobowych obejmuje:

a) ochronę **poufności** danych rozumianej jako zabezpieczenie danych przed dostępem do nich osób nieupoważnionych,
b) ochronę **integralności** rozumianej jako zabezpieczenie danych przed zmianą i zniszczeniem,
c) ochronę **dostępności** rozumianej jako zabezpieczenie danych przed uszkodzeniem, utratą i zniszczeniem.

§ 20

Bezpieczeństwo przetwarzania danych osobowych zapewniają mechanizmy:
a) **uwierzytelniania** (weryfikacji tożsamości użytkownika),
b) **autoryzacji** (określenie uprawnień dostępu użytkownika do informacji),
c) **rozliczalności** (zapis wykonania operacji na danych osobowych) w systemach informatycznych na terenie Urzędu.

Rozdział VI

Odpowiedzialność prawna za naruszenie zasad ochrony danych Osobowych

§ 21

1. Osoby nie przestrzegające przepisów w zakresie ochrony danych osobowych podlegają sankcjom zgodnie z **rozdziałem 8 ustawy o ochronie danych osobowych.**
2. Kto przetwarza dane osobowe lub umożliwia dostęp do nich osobom nieupoważnionym ponosi odpowiedzialność prawną wynikającą z **Kodeksu Karnego i Kodeksu Pracy**.