Załącznik Nr 1
do Zarządzenia Nr .....57...../ 2006
Starosty Raciborskiego
z dnia.....05.12.2006.....

POLITYKA BEZPIECZEŃSTWA

§ 1

Polityka bezpieczeństwa określa obowiązujące w Starostwie Powiatowym w Raciborzu zasady prawidłowego przetwarzania danych osobowych oraz stosowane środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych, określone w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. Nr 101 poz. 926 z 2002 r. z późn. zm.) – zwanej dalej ustawą oraz w przepisach wykonawczych.

§ 2

Dostęp do danych osobowych

1. Dostęp do danych osobowych przetwarzanych w Starostwie Powiatowym może mieć wyłącznie pracownik Starostwa który:
   1) posiada upoważnienie, którego wzór stanowi Załącznik Nr 1 do Polityki Bezpieczeństwa wydane przez Starostę Raciborskiego na wniosek bezpośredniego przełożonego. Wzór wniosku o wydanie upoważnienia do przetwarzania danych osobowych i dostępu do systemu informatycznego stanowi Załącznik Nr 2 do Polityki Bezpieczeństwa
   2) przed przystąpieniem do wykonywania obowiązków służbowych związanych z przetwarzaniem danych osobowych zapoznał się z obowiązującymi zasadami ochrony danych.
      Fakt zaznajomienia się z zasadami udokumentowany jest na formularzu, którego wzór określa Załącznik Nr 3 do Polityki Bezpieczeństwa i przechowywany jest w aktach osobowych pracownika.
   3) w zakresie czynności ma określony:
      a) zakres odpowiedzialności za ochronę tych danych przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem w stopniu odpowiednim do zadań tej osoby przy przetwarzaniu danych.
      b) rodzaj operacji przetwarzania danych, do dokonywania których jest uprawniony w ramach wykonywania czynności służbowych.

2. Wykonywanie czynności przetwarzania danych przez inne osoby (podmioty), nie będące pracownikami Starostwa jest dopuszczalne tylko w razie zawarcia z nimi umowy powierzenia przetwarzania danych osobowych, której wzór stanowi Załącznik Nr 4 do Polityki Bezpieczeństwa.

§ 3

Obowiązki pracownika zatrudnionego przy przetwarzaniu danych osobowych.

Pracownik, który w trakcie wykonywania obowiązków służbowych dokonuje operacji przetwarzania danych osobowych zobowiązany jest do ścisłego przestrzegania obowiązujących przepisów z zakresu ochrony danych osobowych, a w szczególności do:

1) legalnego przetwarzana danych osobowych – zgodnie z art. 23 i 27 ustawy,
2) wykonywania obowiązku informacyjnego – określonego w art. 24 i 25 ustawy
3) zachowania staranności przy przetwarzaniu danych – stosownie do art. 26 i 26 a ustawy
4) realizowania wniosków w zakresie kontroli przetwarzania danych osobowych, zgodnie z art. 32 ustawy
5) zachowania w tajemnicy uzyskanych danych osobowych oraz sposobów ich zabezpieczenia,

§ 4

Udostępnianie danych osobowych

1. Jeżeli przepis szczególny nie stanowi inaczej udostępnianie danych osobowych innej osobie (podmiotowi) niż ta, której dane dotyczą następuje wyłącznie na pisemny wniosek.
Nie jest on obowiązkowy tylko w razie udostępniania danych pomiędzy jednostkami organizacyjnymi Starostwa Powiatowego w Raciborzu.

2. Wniosek, o którym mowa w ust. 1 powinien zawierać:

1) oznaczenie wnioskodawcy;
2) wskazanie podstawy prawnej upoważniającej do uzyskania danych lub posiadanie interesu faktycznego w ich otrzymaniu;
3) oznaczenie osoby, której dane dotyczą;
4) określenie zakresu żądanych danych.

3. Odmowa udostępnienia danych ma formę pisemną z adnotacją o prawie złożenia bezpośrednio do Generalnego Inspektora Danych Osobowych wniosku o wydanie decyzji nakazującej udostępnienie danych.

4. W razie udostępniania danych osobowych przetwarzanych w systemie informatycznym, ma być w nim odnotowywana informacja o odbiorcy danych oraz data i zakres udostępnienia.

§ 5

Miejsca przetwarzania danych osobowych

1. Przetwarzane danych osobowych ma miejsce wyłącznie w pomieszczeniach biurowych Starostwa Powiatowego w Raciborzu..

2. Nie jest dopuszczalne przetwarzanie danych osobowych w komputerach przenośnych.

§ 6

Rejestracja zbiorów danych osobowych

1. Kierownicy jednostek organizacyjnych Starostwa zobowiązani są do:
1) zgłaszania do rejestracji zbiorów danych osobowych oraz zmian w zakresie informacji zawartych w zgłoszonych zbiorach danych.
Zgłoszenia należy dokonywać na formularzu, którego wzór zawiera Załącznik Nr 5 do Polityki Bezpieczeństwa
2) zgłoszenia wykreślenia zbioru danych - w formie pisemnej wraz ze wskazaniem uzasadnienia.

2. Zgłoszenia, o których mowa w ust. 1 należy składać do Kierownika Wydziału Organizacyjnego i Spraw Obywatelskich.

§ 7

Zasady zabezpieczenia danych osobowych przetwarzanych w sposób tradycyjny

1. Dokumenty zawierające dane osobowe przechowywane są w pomieszczeniach biurowych, w meblach zamykanych na klucz.

2. Pomieszczenia biurowe, o których mowa w ust. 1 są:
1) przed rozpoczęciem pracy – sprawdzane, czy nie ma śladów włamania lub uszkodzenia.
Takiemu samemu sprawdzeniu podlegają meble biurowe, w których przechowywane są dokumenty zawierające dane osobowe.
2) w trakcie godzin pracy - zamykane na czas nieobecności osoby zatrudnionej przy przetwarzaniu danych osobowych,
3) po zakończeniu pracy – sprawdzane, czy nie pozostały niezabezpieczone dokumenty zawierające dane osobowe oraz zamknięcie szaf.

3. Osoby nieupoważnione przebywają w pomieszczeniach biurowych tylko w obecności osoby zatrudnionej przy przetwarzaniu danych.

4. Dostęp do zbioru danych osobowych posiada tylko osoba prowadząca zbiór oraz osoba upoważniona.

5. Zasady postępowania z kluczami od pomieszczeń i mebli biurowych określają odrębne przepisy.

6. 1) Do wykonania czynności w zakresie określonym ust. 1 i 2 zobowiązani są pracownicy wykonujący w tych pomieszczeniach biurowych obowiązki służbowe.
2) Nadzór nad przestrzeganiem prawidłowego zabezpieczenia pomieszczeń biurowych i mebli sprawuje Kierownik Wydziału Organizacyjnego i Spraw Obywatelskich

§ 8

Zasady zabezpieczenia danych przetwarzanych w systemie informatycznym.

1.Techniczne zabezpieczenie danych w systemie informatycznym następuje poprzez:
1) autoryzowany dostęp do obsługi stanowiska komputerowego i oprogramowania zgodnie z §3 Instrukcji Zarządzania Systemem Informatycznym stanowiącej Załącznik Nr 2 do Zarządzenia.
2) zabezpieczenie sieci komputerowej, w skład której wchodzą serwery baz danych, serwery internetowe oraz stanowiska komputerowe przed nieautoryzowanym dostępem z sieci INTERNET za pomocą serwera FIREWALL.
3) monitorowanie i rejestrację dostępu z sieci komputerowej do sieci INTERNET oraz rejestrację prób nieautoryzowanego dostępu z sieci INTERNET.
4) skanowanie wszystkich stanowisk komputerowych oprogramowaniem antywirusowym zgodnie z §9 Instrukcji Zarządzania Systemem Informatycznym stanowiącej Załącznik Nr 2 do Zarządzenia.
5) skanowanie poczty elektronicznej przez skaner antywirusowy zainstalowany na serwerze pocztowym.

2.Organizacyjne zabezpieczenie danych w systemie informatycznym następuje poprzez:
1) wyposażenie pomieszczeń z serwerami baz danych w system alarmowy oraz uniemożliwienie dostępu do pomieszczenie z zewnątrz.
2) Zabezpieczenie pomieszczeń ze stanowiskami komputerowymi odbywa się według zasad określonych w §7 ust. 2.

§ 9

Postępowanie w sytuacji naruszenia ochrony danych osobowych

1. W razie stwierdzenia przez osobę zatrudnioną przy przetwarzaniu danych naruszenia ich ochrony (śladów włamania) zobowiązana jest ona do:
1) natychmiastowego powiadomienia o zdarzeniu swojego bezpośredniego przełożonego oraz Administratora Bezpieczeństwa Informacji
2) zabezpieczenia miejsce zdarzenia,
3) fizycznego odłączenia urządzenia i segmentów sieci , które mogły umożliwić dostęp do bazy danych osobom nieupoważnionym.

2. W razie naruszenia ochrony zabezpieczenia danych osobowych przetwarzanych w systemie informatycznym Administrator Bezpieczeństwa Informacji zobowiązany jest do:
1) wylogowania użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych,
2) zmiany hasła na konto administratora i użytkownika poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownego włamania,
3) zapisania wszelkich informacji związanych z danym zdarzeniem a szczególnie czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych lub czas samodzielnego wykrycia tego faktu

4) wygenerowania i wydrukowania (jeżeli zasoby systemu na to pozwalają) wszystkich możliwych dokumentów i raportów, które mogą pomóc w ustaleniu okoliczności zdarzenia. Należy opatrzyć je datą i podpisem,
4) sprawdzenia:
a) stanu urządzeń wykorzystywanych do przetwarzania danych osobowych,
b) zawartości zbioru danych,
c) sposobu działania programu,
d) jakości komunikacji w sieci telekomunikacyjnej,
c) wykluczenia możliwości obecności wirusów komputerowych
5) przystąpienia do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali szkód i sposobu dostępu do danych osoby niepowołanej.

3. Administrator Bezpieczeństwa Informacji sporządza protokół ze stwierdzonego naruszenia ochrony danych osobowych zawierający w szczególności:
1) rodzaj zaistniałego zdarzenia,
2) dokładny czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych,
3) określenie sposobu naruszenia zabezpieczenia ochrony danych osobowych,
4) określenie ewentualnych szkód lub zniszczeń,
5) określenie przyczyny naruszenia danych osobowych.

Protokół sporządza się w terminie 14 dni od daty zaistnienia zdarzenia i przekazuje Staroście Raciborskiemu.

§ 10

Kontrola stosowania zasad przetwarzania danych osobowych

1. Przedmiotem kontroli stosowanych zabezpieczeń danych osobowych jest sprawdzenie:
1) konfiguracji sprzętowo-programowej,
2) zabezpieczeń programowych i sprzętowych (aktualny identyfikator, hasło),
3) prawidłowego ustawienia monitora w biurze,
4) prawidłowości przestrzeganie procedury udostępniania danych osobowych.
5) aktualizowania programu antywirusowego,
6) przeglądanych stron internetowych,
7) zabezpieczenia szaf, pomieszczeń biurowych w którym przechowywane są dane osobowe,

2. Kontrolę w zakresie określonym w:
1) ust. 1 pkt. 1-6 – przeprowadza Koordynator spraw związanych z ochroną danych osobowych i Administrator Bezpieczeństwa Informacji.
2) ust. 1 pkt. 7 - przeprowadza Koordynator spraw zawiązanych z ochroną danych osobowych i Kierownik Wydziału Organizacyjnego i Spraw Obywatelskich

3. Sposób ustalania harmonogramu kontroli oraz zasady dokumentowania jej wyników określają przepisy odrębne

§ 11

Postanowienia końcowe

1. Koordynator spraw związanych z ochroną danych osobowych odpowiedzialny jest w szczególności za:
   1) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych w Starostwie Powiatowym według wzoru określonego w Załączniku Nr 6 do Polityki Bezpieczeństwa.
   2) zgłaszanie do rejestracji przez Generalnego Inspektora Ochrony Danych Osobowych zbiorów danych osobowych oraz prowadzenie ich wykazu.
      Wykaz zbiorów danych osobowych zgłoszonych do rejestracji przez Generalnego Inspektora Danych Osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych stanowi Załącznik Nr 7 do Polityki Bezpieczeństwa.

2. Administrator Bezpieczeństwa Informacji odpowiedzialny jest za:
   1) prowadzenie dokumentacji opisującej sposób przetwarzania danych w systemie informatycznym.
      Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi stanowi Załącznik Nr 8 do Polityki Bezpieczeństwa.
   2) wprowadzenie i kontrolowanie stosowania zabezpieczeń danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy, uszkodzeniem lub zniszczeniem
   3) stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednia do zagrożeń oraz kategorii danych objętych ochroną
   4) wprowadzenie i nadzór realizacji obowiązków w zakresie fizycznego zabezpieczenia urządzeń i nośników
   5) określenie i nadzór nad stosowaniem wymogów w zakresie struktur baz danych i aplikacji nimi zarządzających;
   6) wprowadzenie i nadzór nad kompleksowym systemem uwierzytelniania użytkowników.
   7) podejmowanie działań w razie wykrycia naruszeń w systemie informatycznym,
   8) prowadzenie szkoleń pracowników w zakresie stosowanych środków zabezpieczenia danych osobowych w systemie informatycznym
   9) prowadzenie ewidencji stanowisk komputerowych i osób odpowiedzialnych za ich użytkowanie zgodnie z Instrukcją Zarządzania Systemem Informatycznym, stanowiącej Załącznik Nr 2 do Zarządzenia