Załącznik Nr 2
do Zarządzenia Nr.....57...../ 2006
Starosty Raciborskiego
z dnia.....05.12.2006.....

Instrukcja
zarządzania systemem informatycznym
Starostwa Powiatowego w Raciborzu

§ 1

Instrukcja zarządzania systemem informatycznym ma na celu określenie obowiązujących w Starostwie Powiatowym zasad ochrony danych osobowych przetwarzanych w systemie informatycznym, w szczególności zapewnienie bezpieczeństwa ich przetwarzania.

§ 2

Identyfikacja zagrożeń w przetwarzaniu danych.

Bezpieczeństwo przetwarzanych danych osobowych, a szczególnie ich poufność, rozliczalność oraz integralność narażona jest przez:
1) włamanie do systemu informatycznego i pozyskanie danych przez osoby nieuprawnione;
2) pozyskanie danych przez osoby nieuprawnione na skutek bezpośredniego dostępu do komputera;
3) pozyskanie danych osobowych w trakcie przesyłania ich drogą internetową;
4) dokonywanie modyfikacji danych przez osoby nieuprawnione.

§ 3

Przydział uprawnień dostępu do systemu informatycznego.

1. Każdy użytkownik systemu informatycznego posługuje się przyznanym identyfikatorem i hasłem.
1) Identyfikator wraz hasłem przyznawany jest na wniosek , o którym mowa w Załączniku Nr 2 do Polityki Bezpieczeństwa, bezpośredniego przełożonego i uprawnia do obsługi konkretnego systemu.
2) Uprawnienia dostępu do systemu są odbierane w chwili zwolnienia pracownika, co Administrator Bezpieczeństwa Informacji potwierdza w karcie obiegowej pracownika.

3) Uprawnienia dostępu do systemu mogą być odebrane lub zablokowane także na pisemny wniosek bezpośredniego przełożonego lub przez Administratora Bezpieczeństwa Informacji w razie stwierdzenia niewłaściwego użytkowania systemu informatycznego.

2. Identyfikator :
1) jest nazwą użytkownika (jednoznacznie go identyfikuje) w systemie informatycznym na poziomie systemu operacyjnego.
2) składa się z unikalnego i niepowtarzalnego ciągu znaków literowo-cyfrowych,
3) nie może być zmieniony bez wiedzy użytkownika;
4) nie będzie nigdy przyznany innemu użytkownikowi

3. Hasło:
1) powinno być znane tylko osobie, która się nim posługuje. W przypadku powstania podejrzenia o możliwości poznania hasła przez inne osoby należy je natychmiast zmienić;
2) pierwsze hasło użytkownika jest identyczne z nazwą użytkownika; po pierwszym zalogowaniu do programu użytkownik winien zmienić hasło wg zasad nadawania haseł określonym w programie.
3) musi być zmieniane przez użytkownika co miesiąc;

4. Za przydział identyfikatorów i haseł odpowiedzialny jest Administrator Bezpieczeństwa Informacji.

5. Zabronione jest :
1) zapisywanie identyfikatorów i haseł w miejscach ogólnodostępnych.
2) przekazywania identyfikatorów i haseł użytkowników innym osobom.

§ 4

Zasady obowiązujące użytkownika w trakcie pracy w systemie

1. Rozpoczęcie pracy w systemie informatycznym następuje przez zalogowanie się poprzez podanie identyfikatora użytkownika i hasła dostępu.
2. W czasie pracy (przerw w korzystaniu z systemu) przed odejściem od komputera należy się wyrejestrować z systemu.
3. Zakończenie pracy w systemie następuje przez wydanie polecenia systemowego kończącego sesję z użytkownikiem i wyłączeniu wszystkich urządzeń.
4. Zabrania się wyłączania komputera bez poprawnego wyrejestrowania.

§ 5

Tworzenie kopii awaryjnych baz danych

1. Kopie awaryjne oprogramowania sieciowego wykonuje Administrator Bezpieczeństwa Informacji.
2. Kopie awaryjne, o których mowa w ust. 1:
1) wykonywane są codziennie od poniedziałku do czwartku po godzinach pracy urzędu, na osobnych nośnikach;
2) wykorzystane są dwa komplety nośników danych. W dniach poprzedzających okres wolny od pracy (piątki, święta) kopie awaryjne nie będą wykonywane.
3) deponowane są w oddzielnym pomieszczeniu. Za prawidłowe zabezpieczenie nośników odpowiada wyznaczony przez Administratora Bezpieczeństwa Informacji pracownik
4) komplet nośników awaryjnych wymieniany jest co 6 miesięcy; uszkodzone nośniki podlegają zniszczeniu.

3. Kopie awaryjne danych przetwarzanych na komputerach PC (komputery jednostanowiskowe) tworzone są przez użytkownika.

4. Kopie awaryjne, o których mowa w ust. 3 są:
1) wykonywane codziennie,
2) przechowywane na dyskietkach przez użytkownika stanowiska,
3) okresowo sprawdzane pod kątem ich dalszej przydatności do odtworzenia,
4) poddawane bezzwłocznemu usunięciu po ustaniu ich użyteczności,
5) archiwizowane na serwerze sieciowym w udostępnionym przez Administratora Bezpieczeństwa Informacji katalogu.

§ 6

Sposób zabezpieczenia nośników danych.

1. Nośniki informacji muszą być:
1) składowane w zamykanych meblach biurowych;
2) zabezpieczone przed zabraniem przez osobę nieuprawnioną;
3) przed likwidacją pozbawione zapisu danych, a jeśli jest to niemożliwe nośnik należy uszkodzić w sposób uniemożliwiający odczytanie.

2. Nośniki zawierające kopie zapasowe, o których mowa w §5 ust. 1 niniejszej Instrukcji, w każdy ostatni dzień pracy w tygodniu, przekazywane są do zdeponowania w oddzielnym pomieszczeniu za pośrednictwem wskazanej osoby.

§ 7

Wydruki komputerowe

1. Wykonywanie wydruków komputerowych zawierających dane osobowe na drukarce systemowej lub stanowiskowej odbywają się pod kontrolą osoby wykonującej wydruk.
2. Wszystkie wydruki zawierające dane osobowe przeznaczone do zniszczenia należy zniszczyć w niszczarkach dokumentów.

§ 8

Przeglądy i konserwacja sprzętu komputerowego

1. Użytkownicy systemu komputerowego zgłaszają Administratorowi Bezpieczeństwa Informacji wszelkie awarie sprzętu komputerowego.
2. W przypadku stwierdzenia awarii sprzętu zawierającego dane osobowe:
1) naprawa i konserwacja sprzętu winna odbyć się na miejscu;
2) naprawa uszkodzenia informacji dotyczących baz danych osobowych winna odbyć się na miejscu.
3) w razie konieczności dokonania naprawy w serwisie Administrator zabezpiecza dane poprzez wymontowanie nośnika danych lub nadzoruje naprawę.
3. Z firmą lub instytucją zewnętrzną przeprowadzającą naprawy należy podpisać umowę o powierzenie przetwarzania danych.

Wzór umowy o powierzenie przetwarzanie danych osobowych stanowi Załącznik Nr 4 do Polityki Bezpieczeństwa.

§ 9

Ochrona i zasady korzystania z komputerów PC.

1. Ochrona komputerów PC przed wirusami komputerowymi:
1) Administratora Bezpieczeństwa Informacji instaluje na każdym stanowisku komputerowym oprogramowanie antywirusowe.
2) za bezpieczeństwo antywirusowe odpowiada użytkownik komputera.
3) zabrania się używania dyskietek nie sprawdzonych na obecność wirusów komputerowych.
4) należy codziennie aktualizować oprogramowanie antywirusowe i skanować dyski komputera programem anrtywirusowym.
5) fakt znalezienia wirusa należy zgłaszać administratorowi systemu informatycznego.
6) zabrania się samodzielnego instalowania oprogramowania bez wiedzy administratora systemu

informatycznego.
7) zabrania się przeglądania stron internetowych nie związanych z wykonywanymi czynnościami służbowymi.
8) zabrania się udostępniania w sieci komputerowej zasobów komputera zawierających dane osobowe.

2. Ochrona komputerów PC przed nieautoryzowanym dostępem do systemu informatycznego następuje poprzez:
1) 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.
2) 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.
5) skanowanie poczty elektonicznej przez skaner antywirusowy zainstalowany na serwerze pocztowym.

3. Instalacja oprogramowania komputerowego.
1) Instalacji oprogramowania na stanowiskach komputerowych dokonuje wyłącznie pracownik zatrudniony na stanowisku ds. komputeryzacji Starostwa Powiatowego;
2) każde oprogramowanie przed zainstalowaniem na stanowisku komputerowym PC podlega rejestracji przez pracownika zatrudnionego na stanowisku ds. komputeryzacji Starostwa Powiatowego,
3) zabrania się użytkownikom stanowisk komputerowych:
a) instalowania i użytkowania nielegalnego oprogramowania,
b) przechowywania kopii nielegalnego oprogramowania,
c) instalowania oprogramowania nie przeznaczonego do wykonywania obowiązków służbowych,
d) deinstalowania zainstalowanego na stanowisku komputerowym oprogramowania,
e) przeinstalowania oprogramowania na inne stanowisko,

4. Użytkowanie sprzętu komputerowego
1) za każde stanowisko komputerowe znajdujące się w Starostwie odpowiedzialny jest wyznaczony przez Starostę Raciborskiego pracownik,
2) zabrania się użytkownikom stanowisk komputerowych:
a) samodzielnego instalowania lub demontowania zainstalowanego osprzętu,
b) podłączania do sieci komputerowej sprzętu komputerowego nie będącego własnością Starostwa,
c)dokonywania samodzielnych napraw sprzętu,
d) dokonywania samodzielnych zmian miejsca użytkowania sprzętu
3) wszelkie awarie sprzętu należy zgłaszać pracownikowi zatrudnionemu na stanowisku ds. komputeryzacji Starostwa ,
4) instalację sprzętu komputerowego na stanowisku pracy wykonuje wyłącznie pracownik zatrudniony na stanowisku ds. komputeryzacji Starostwa.

5. Administrator systemu informatycznego prowadzi rejestr sprzętu i oprogramowania użytkowanego w Starostwie Powiatowym.

§ 10

Oprogramowanie przetwarzające dane osobowe powinno umożliwiać rejestrację informacji o odbiorcach danych osobowych, dacie i zakresie ich udostępnienia.

STAROSTA
Adam Hajduk