Załącznik nr 2
Do Zarządzenia nr ....25.../.2003.
Starosty Poznańskiego
Z dnia .22.09.2003r.

Instrukcja określająca sposób zarządzania systemem informatycznym Starostwa Powiatowego w Poznaniu.

Starostwo Powiatowe w Poznaniu

STAROSTA POZNAŃSKI
.....Jan Grabkowski.....
Starosta

Opracował:

Marek Jóźwiak
Piotr Siwczak

§ 1

Podstawę prawną do niniejszej instrukcji stanowią:
1) ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883),
2) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przechowywania danych osobowych (Dz. U. Nr 80, poz. 521),
3) regulamin ochrony danych osobowych w Starostwie Powiatowym w Poznaniu

§ 2

Instrukcja zarządzania systemami informatycznymi w Starostwie Powiatowym w Poznaniu ma na celu osiągnięcie i utrzymywanie odpowiedniego poziomu poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności systemu.

Administrator danych przed przystąpieniem do przetwarzania danych osobowych w systemie informatycznym określa:
- *cele, strategię i politykę bezpieczeństwa systemu informatycznego w firmie,*
- *identyfikuje i analizuje zagrożenia dla zasobów informatycznych, - identyfikuje i analizuje ryzyko,*
- *monitoruje wdrożenie i eksploatację zabezpieczeń w celu racjonalnej ochrony informacji,*
- *opracowuje program uświadamiania w zakresie bezpieczeństwa oraz prowadzi szkolenia,*
- *wykrywa i reaguje na incydenty.*

Celem polityki bezpieczeństwa systemu informatycznego jest zapewnienie poufności danych osobowych i informacji niejawnych w nim się znajdujących. Prawidłowe zarządzanie zasobami informatycznymi jest głównym obowiązkiem osób odpowiedzialnych za kierowanie Starostwem na wszystkich poziomach.

Zasoby informatyczne to:
- zasoby fizyczne - sprzęt komputerowy, urządzenia komunikacyjne, budynki.
- informacje - baza danych,
- oprogramowanie,
- pracownicy.

Zasoby podlegają wielu rodzajom zagrożeń. Zagrożenia mogą być potencjalną przyczyną incydentu, który może spowodować szkodę dla systemu Starostwa i jego zasobów. Szkoda może powstać na skutek uszkodzenia, ujawnienia, modyfikacji, utraty informacji lub jej dostępności. Zadaniem administratora jest zidentyfikowanie zagrożeń przypadkowych, rozmyślnych, określenie ich poziomu i prawdopodobieństwa oraz zapobieganie ich powstaniu. Odpowiedni dobór zabezpieczeń jest kluczowy dla prawidłowego wdrożenia polityki bezpieczeństwa. Zabezpieczenia obejmują: ochronę budynków. sprzętu komputerowego. oprogramowania, wprowadzone mechanizmy kontroli dostępu, hasła, oprogramowanie antywirusowe. zasilanie rezerwowe. kopie zapasowe.

Uświadamianie w zakresie bezpieczeństwa obejmuje szkolenie pracowników.

Zarządzanie sprzętem informatycznym jest trwałym procesem w Starostwie, składającym się z zarządzania konfiguracją,. zarządzania zmianami, ryzykiem i monitorowaniem, uświadamianiem w zakresie bezpieczeństwa, analizą ryzyka.

- zarządzanie konfiguracją to proces śledzenia zmian w systemie. Podstawowym zadaniem jest zapewnienie. aby zmiany w systemie nie obniżały efektywności zabezpieczeń i całkowitego bezpieczeństwa Starostwa;

- zarządzanie zmianami jest procesem używanym w Starostwie w celu identyfikacji nowych wymagań bezpieczeństwa, gdy następują zmiany w systemie informatycznym, polegające na wprowadzeniu zmian sprzętowych. aktualizacji oprogramowania, nowych użytkowników, dodatkowych połączeń sieciowych;

- zarządzanie ryzykiem w Starostwie jest wykonywane podczas całego okresu pracy systemu. Dotyczy projektowania i rozwoju systemu. Analiza systemu informatycznego składa się z analizy wartości zasobów. zagrożeń i podatności na zagrożenia. Jej wynikiem jest określenie prawdopodobnego ryzyka dla zasobów.

-skuteczne zabezpieczenia wymagają rozliczalności i bezpośredniego przyjęcia do wiadomości obowiązków z zakresu bezpieczeństwa. Zadanie to jest realizowane w Starostwie poprzez szkolenia pracowników;

-monitorowanie obejmuje okresową kontrolę sprzętu oraz regularną analizę logów w systemie informatycznym pod kątem naruszenia zabezpieczeń;

-planowanie awaryjne dotyczy zabezpieczeń związanych z awarią sprzętu.

Dla realizacji zadań związanych z zarządzaniem systemem informatycznym w Starostwie Powiatowym zatrudniony jest administrator sieci (tel. 521), a ponadto powołano administratora bezpieczeństwa informacji. Do szczegółowych obowiązków administratora bezpieczeństwa informacji należy:

1) określenie sposobu przydziału haseł dla użytkowników i częstotliwości ich zmiany oraz wskazanie osoby odpowiedzialnej za te czynności,

2) określenie sposobu rejestrowania i wyrejestrowywania użytkowników oraz wskazanie osoby odpowiedzialnej za te czynności.

3) procedury rozpoczęcia i zakończenia pracy,

4) metoda i częstotliwość tworzenia kopii awaryjnych,

5) metoda i częstotliwość sprawdzania obecności wirusów komputerowych oraz metoda ich usuwania,

6) sposób i czas przechowywania nośników informacji. w tym kopii informatycznych i wydruków,

7) sposób dokonywania przeglądów i konserwacji systemu oraz zbiory danych osobowych,

8) sposób postępowania w zakresie komunikacji w sieci komputerowej.

§ 3

1) Wszyscy pracownicy Starostwa mający dostęp, nawet w ograniczonym zakresie, do danych osobowych muszą zapoznać się z ustawą o ochronie danych osobowych, rozporządzeniami wykonawczymi. regulaminem oraz instrukcjami. Fakt przeszkolenia pracownicy potwierdzają swoim podpisem.
2) Dostęp do pomieszczeń. w których odbywa się przetwarzanie i przechowywanie danych osobowych. mają upoważnione osoby zatrudnione w Starostwie, po uprzednim zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych. Listę osób mających upoważnienie do przebywania w pomieszczeniach, w których

odbywa się przechowywanie i przetwarzanie danych. tworzy w imieniu administratora danych, administrator bezpieczeństwa informacji.
3) Osoby nie będące pracownikami Starostwa mogą przebywać wewnątrz obszaru, w którym odbywa się przetwarzanie i przechowywanie danych. jedynie w obecności osoby zatrudnionej w Starostwie i za zgodą administratora danych.
4) W przypadku istnienia możliwości technicznych (obszar monitorowany – Wydział Komunikacji i Transportu), administrator bezpieczeństwa informacji sprawdza. w cyklu tygodniowym. zdarzenia wejścia i wyjścia z obszarów przechowywania i przetwarzania danych osobowych.

§ 4

1) **Dostęp do sieci komputerowej** oraz serwera plików, na którym przechowywane są dane osobowe w postaci elektronicznej, zabezpieczony jest systemem użytkowników, haseł oraz kontrolą dostępu do określonych zasobów.
2) **Wykaz użytkowników** wraz z zakresem dostępu tworzony jest przy współudziale administratora sieci komputerowej, przez administratora bezpieczeństwa informacji.
3) **Hasła dostępu** dla poszczególnych użytkowników zasobów informatycznych Starostwa zmieniane są automatycznie. w cyklu miesięcznym.

§ 5

W przypadku przetwarzania danych osobowych na stacjonarnych komputerach nie mających połączenia z serwerem plików oraz na komputerach przenośnych. stosuje się następujące procedury zabezpieczeń:
1) dostęp do komputerów mają tylko upoważnieni pracownicy i jest zabezpieczony hasłem,
2) dane na komputery przenoszone są przez upoważnionych pracowników ;
- w przypadku komputera przenośnego - bezpośrednio z serwera plików,
- w przypadku komputera stacjonarnego - za pomocą dyskietek,
3) po skończeniu przetwarzania danych wszelkie informacje muszą być wymazywane z pamięci komputerów.

§ 6

1) Dostęp do aplikacji bazy danych ustala administrator bezpieczeństwa informacji,
2) Uprawniony użytkownik - pracownik Starostwa, przydzielany ma identyfikator, hasło i poziom uprawnień.
3) W przypadku, gdy pracownik traci prawo do przetwarzania danych osobowych. nie usuwa się jego identyfikatora. Administrator bezpieczeństwa informacji usuwa jedynie uprawnienia do korzystania z aplikacji oraz wraz z administratorem sieci komputerowej odbiera możliwość korzystania z dostępu do obszaru dysku sieciowego, na którym znajdują się dane osobowe.

§ 7

1) Pracownik zatrudniony przy przetwarzaniu danych osobowych loguje się do sieci komputerowej, Po zaakceptowaniu przez system jego identyfikatora oraz hasła. uruchamia aplikację. służącą do przetwarzania i przechowywania danych osobowych,

2) W przypadku opuszczenia. nawet na chwilę. stanowiska pracy (opuszczenie pomieszczenia). pracownik jest zobowiązany zablokować nieautoryzowany dostęp do stacji roboczej.
3) Po zakończeniu pracy pracownik jest zobowiązany opuścić aplikację oraz wyłączyć terminal umożliwiający przetwarzanie danych.

§ 8

1) Skanowanie dysków komputerowych na obecność wirusa komputerowego musi się odbywać co najmniej raz w tygodniu. za pomocą specjalnego programu antywirusowego. Ochronę zasobów informatycznych przed zainfekowaniem wirusem komputerowym sprawuje administrator sieci komputerowej,
2) Wprowadza się zakaz instalowania jakiegokolwiek oprogramowania na dyskach komputerów przez pracowników Starostwa.
3) Dane z zewnątrz (za pomocą dyskietek lub sieci komputerowej) pobierać mogą jedynie upoważnieni pracownicy, po uprzednim zeskanowaniu plików lub nośników informacji na obecność wirusa komputerowego.

§ 9

Wszelkie wydruki z systemów informatycznych, zawierające informacje niejawne lub dane osobowe, muszą być przechowywane w zabezpieczonych siedzibach Starostwa.

§ 10

1) Aplikacja służąca do przetwarzania i przechowywania danych osobowych zawiera procedury umożliwiające kontrolę pracy systemu oraz prawidłowość zapisów danych. Administrator bezpieczeństwa informacji lub upoważniona przez niego osoba, powinna uruchamiać procedury kontrolne przynajmniej raz w miesiącu.
2) Za jakość sprzętu komputerowego, sieci komputerowej oraz jego okresową konserwację odpowiada administrator sieci komputerowej.

§ 11

W przypadku awarii systemu komputerowego i utraty informacji lub w przypadku domniemania, że informacja uległa uszkodzeniu należy przedsięwziąć następujące środki:
1) przetestować sieć komputerową oraz pracę aplikacji służącej do przetwarzania i przechowywania danych osobowych,
2) wykorzystać ostatnią kopię awaryjną do odtworzenia danych osobowych,
3) w przypadku, gdy nie można odtworzyć ostatniej kopii lub istnieje podejrzenie, że zawiera dane uszkodzone, wykorzystać ostatnią sprawną kopię bezpieczeństwa.

§ 12

Administrator bezpieczeństwa informacji zobowiązany jest do przeprowadzania okresowej analizy zagrożeń, podatności na zagrożenia oraz wartości zasobów.

§ 13

Niniejsza instrukcja wchodzi w życie z dniem zgłoszenia bazy danych do Generalnego Inspektora Ochrony Danych Osobowych.

STAROSTA POZNAŃSKI

Jan Grabkowski