ZARZĄDZENIE NR 2/2005

Starosty Łódzkiego Wschodniego

z dnia 03 stycznia 2005r.

w sprawie ustalenia Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Starostwie Powiatowym w Łodzi.

Na podstawie § 3 ust. 1, w związku z § 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r., w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, zarządza się, co następuje:

§ 1. Ustala się Instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Starostwie Powiatowym w Łodzi, stanowiącą załącznik do niniejszego Zarządzenia.

§ 2. Instrukcja, o której mowa w § 1 niniejszego Zarządzenia nie dotyczy:
1) Systemu do elektronicznego przesyłania danych do produkcji praw jazdy (SPD) oraz
2) Systemu centralnej personalizacji dowodów rejestracyjnych – system „Pojazd", których użytkownikiem jest Wydział Komunikacji i Spraw Obywatelskich.

§ 3. Zarządzanie systemami informatycznymi wyszczególnionymi w § 2 niniejszego Zarządzenia określają następujące instrukcje:
1) Instrukcja Bezpieczeństwa systemu transmisji danych do produkcji praw jazdy oraz
2) Instrukcja Bezpieczeństwa Systemu „Pojazd" w Urzędzie

ustalone przez Polską Wytwórnię Papierów Wartościowych S.A. w Warszawie.

§ 4. Administratora bezpieczeństwa informacji zobowiązuje się do zapoznania z postanowieniami Instrukcji ustalonej niniejszym Zarządzeniem pracowników Starostwa Powiatowego w Łodzi obsługujących systemy informatyczne służące do przetwarzania danych oraz do sprawowania kontroli w zakresie przestrzegania zawartych w Instrukcji uregulowań.

§ 5. Traci moc Zarządzenie Nr 22/99 Starosty Łódzkiego Wschodniego z dnia 28 października 1999r. w sprawie instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych oraz instrukcji określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

§ 6. Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA

Andrzej Opala

Załącznik
do Zarządzenia Nr 2/2005
Starosty Łódzkiego Wschodniego
z dnia 03 stycznia 2005r.

Instrukcja
zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Starostwie Powiatowym w Łodzi

§ 1.

Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.

1. Osobą odpowiedzialną za rejestrowanie i wyrejestrowane użytkowników w jednostce jest administrator bezpieczeństwa informacji.
2. Podstawą do zarejestrowania użytkownika do danego systemu przetwarzania danych jest upoważnienie nadane przez administratora danych. Natomiast podstawą do wyrejestrowania użytkownika z danego systemu przetwarzania danych jest cofnięcie upoważnienia lub ustanie zatrudnienia.
3. Administrator bezpieczeństwa informacji rejestruje oraz wyrejestrowuje użytkowników, prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych archiwizując identyfikator, imię i nazwisko użytkownika.
4. Identyfikatory osób, które utraciły uprawnienia dostępu do danych, należy wyrejestrować z systemu, unieważniając przekazanie hasła, identyfikator po wyrejestrowaniu użytkownika nie jest przydzielany innej osobie.
5. Osoby upoważnione do przetwarzania danych obowiązane są do zachowania w tajemnicy tych danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje również po ustaniu zatrudnienia.

§ 2

Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem.

1. Przekazywanie haseł odbywa się w formie pisemnej.
2. Hasło powinno składać się co najmniej z 6 znaków.
3. Osobą odpowiedzialną za przydzielanie haseł jest administrator bezpieczeństwa informacji.
4. Hasła nie mogą być przekazywane przez osoby trzecie lub za pośrednictwem niechronionych wiadomości poczty elektronicznej.
5. Użytkownik po otrzymaniu hasła jest obowiązany do niezwłocznej jego zmiany, chyba że system nie umożliwia wykonania takiej operacji.
6. Hasło nie może się powtarzać częściej niż raz w roku, powinno zawierać minimalnie 6 znaków, może być stosowany zestaw haseł zawierający większą ilość znaków specjalnych, małe i wielkie litery oraz cyfry.
7. Zmiana hasła jest wymuszona przez system po 30 dniach.
8. Hasła w systemie są przechowywane w postaci zaszyfrowanej.
9. Tworzony jest rejestr logowań wszystkich użytkowników oraz administratorów systemu.

§ 3

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.

1. Użytkownicy przed przystąpieniem do pracy przy przetwarzaniu danych powinni zwrócić uwagę, czy nie istnieją przesłanki do tego, że dane zostały naruszone. Jeżeli istnieje takie podejrzenie, należy niezwłocznie powiadomić administratora bezpieczeństwa informacji.
2. Dostęp do określonego zasobów danych jest możliwy dopiero po podaniu właściwego identyfikatora i hasła dostępu.
3. Hasło użytkownika należy podawać do systemu w sposób dyskretny (nie literować, nie czytać na głos, wpisywać osobiście, nie pozwalać na bezpośrednią obecność drugiej osoby podczas wpisywania hasła, itp..
4. Użytkownik ma obowiązek zamykania systemu, programu komputerowego po zakończeniu pracy lub przed wyłączeniem stacji komputerowej.
5. Stanowisko komputerowe z uruchomionym systemem, programem nie może pozostawać bez kontroli pracującego na nim użytkownika.
6. Pomieszczenia, w których znajdują się urządzenia służące do przetwarzania danych oraz wydruki lub inne nośniki zawierające dane, winny być zamknięte na dwa zamki, z których co najmniej jeden jest atestowany.

§ 4.

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

1. Kopia zapasowa tworzona jest na dysku serwera raz dziennie przed zakończeniem pracy systemu.
2. Metoda sporządzania kopii zapasowych to „kopia całościowa"
3. Poszczególne kopie dzienne są przenoszone na dyski optyczne raz w tygodniu.
4. Kopie zapasowe przechowuje się w miejscu zabezpieczającym je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.
5. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, należy pozbawić zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadzać w sposób uniemożliwiający ich odczytanie.

§ 5.

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych zbiorów danych.

1. Elektroniczne nośniki informacji oraz kopie zapasowe zbiorów danych zapisane na nośnikach należy przechowywać w szafie pancernej.
2. Elektroniczne nośniki informacji oraz kopie zapasowe zbiorów danych zapisane na nośnikach usuwa się niezwłocznie po ustaniu ich użyteczności.

§ 6.

Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu lub utratą danych spowodowaną awarią zasilania, lub zakłóceniami w sieci zasilającej.

1. Dopuszcza się łączenie z siecią internetu i używanie poczty elektronicznej tylko na zestawach komputerowych, w których nie przetwarza się danych osobowych.
2. Zabrania się przesyłania danych na zewnątrz za pośrednictwem internetu (poczty elektronicznej).
3. Dopuszcza się używanie nośników danych z zewnątrz (dyskietek, płyt CD, innych urządzeń magnetycznych) na komputerach, w których przetwarzane dane wyłącznie po uprzednim sprawdzeniu przez administratora bezpieczeństwa informacji, w celu wyeliminowania wszelkich zagrożeń.

4. Urządzenia i systemy informatyczne powinny być zabezpieczone przed utratą danych, spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez stosowanie zasilaczy UPS.
5. Pomieszczenia, w których przetwarzane są dane osobowe powinny posiadać odpowiednio zabezpieczone okna i drzwi wejściowe.
6. Pomieszczenia, w których przetwarzane są dane osobowe powinny być zabezpieczone przed pożarem.
7. Oprogramowanie winno być instalowane przez administratora bezpieczeństwa informacji lub pod jego nadzorem.

§ 7.

Informacje odnotowywane w systemach informatycznych służących do przetwarzania danych osobowych oraz sposób ich odnotowywania.

1. Dla każdej osoby, której dane osobowe są przetwarzane w systemach informatycznych zapewniane są odnotowania:
   1) daty pierwszego wprowadzenia danych do sytemu;
   2) identyfikatora użytkownika wprowadzającego dane;
   3) źródła danych, w przypadku zbierania danych, nie od osoby, której dotyczą;
   4) informacje o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia;
   5) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.
2. Odnotowanie informacji następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.
3. System zapewnia sporządzenie i wydrukowanie raportu zawierającego dane dla każdej osoby, której dane dotyczą.

§ 8.

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

1. Przeglądy dokonywane są w celu oceny stanu technicznego urządzeń (komputery, serwery, UPS-y, itp.), stanu okablowania budynku w sieć logiczną, spójności baz danych, stanu zabezpieczeń fizycznych (zamki, kraty), stanu rejestrów systemowych serwera, lokalnej sieci komputerowej.
2. Przeglądów i konserwacji systemów przetwarzania danych dokonuje administrator bezpieczeństwa informacji co najmniej raz w miesiącu.
3. W przypadku przekazywania do naprawy nośników informatycznych zawierających dane osobowe należy, gdy tylko to możliwe usunąć wszystkie informacje na nich zapisane, przed ich przekazaniem, bądź też naprawić je pod nadzorem osoby upoważnionej przez administratora danych.

§ 9.

Tryb postępowania w sytuacji naruszenia danych osobowych przetwarzanych w systemach informatycznych.

1. W sytuacji naruszenia zabezpieczenia danych osobowych w systemach informatycznych bądź sytuacji mogącej wskazać na naruszenie zabezpieczeń tych danych, osoba przetwarzająca dane osobowe jest obowiązana niezwłocznie powiadomić o tym administratora bezpieczeństwa informacji.
2. Administrator bezpieczeństwa informacji obowiązany jest
   1) zidentyfikować rodzaj zaistniałego zdarzenia, określić skalę zniszczeń i metody dostępu do danych osobowych osoby nieuprawnionej;
   2) podjąć działania w celu powstrzymania lub ograniczenia dostępu do danych osoby nieuprawnionej, zminimalizowanie szkód;

3) przeprowadzić wstępną analizę stanu systemu, w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych w systemie;
4) Przeprowadzić analizę stanu systemu informatycznego, o ile zaistniał fakt naruszenia ochrony danych, a następnie przywrócić normalny stan działania systemu.

STAROSTA

Andrzej Opala