Załącznik nr 1
do Zarządzenia Starosty Lęborskiego z dnia 28 lipca 1999 r.
w sprawie zarządzania bezpieczeństwem zbiorów
danych osobowych oraz ochrony tychże danych
przetwarzanych w Starostwie Powiatowym w Lęborku

Program szkolenia na temat zabezpieczenia zbiorów danych osobowych

1. Omówienie celów, strategii i zabezpieczeń systemów informatycznych, w których przetwarzane są dane oraz zabezpieczeń zbiorów prowadzonych w formie tradycyjnej (kartotekach, księgach, wykazach, i innych zbiorach ewidencyjnych),

2. Omówienie zagrożeń i ryzyka, na które może być narażone przetwarzanie danych osobowych.

3. Omówienie zasad przetwarzania danych osobowych:
   a) obowiązek informowania osób, których dane dotyczą - wynikający z art. 24 i 25 ustawy o ochronie danych osobowych,
   b) omówienie praw osoby, której dane dotyczą,
   c) przetwarzanie danych zwykłych,
   d) przetwarzanie danych wrażliwych,
   e) przetwarzanie danych o karalności.

4. Poinstruowanie o sposobie postępowania w sytuacji naruszenia baz danych osobowych.

5. Omówienie sposobu zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji:
   a) procedury rozpoczęcia i zakończenia pracy,
   b) sposoby zabezpieczeń pomieszczeń oraz nośników informacji,
   c) sposoby przechowywania nośników informacji,
   d) sposoby wykonywania, przechowywania i niszczenia wydruków,
   e) sposoby postępowania w zakresie komunikacji sieciowej,
   f) sposoby pozbawiania nośników informacji przeznaczonych do likwidacji lub naprawy danych osobowych,
   g) odtwarzanie danych z kopii awaryjnych oraz sprawdzanie ich pod kątem dalszej przydatności do odtworzenia danych w przypadku awarii,
   h) sposoby i częstotliwość wprowadzania haseł.

6. Omówienie sposobu zarządzania zbiorami danych osobowych prowadzonych w formie tradycyjnej,

7. Omówienie zasad udostępniania danych osobowych:
   a) pisemny umotywowany wniosek,
   b) inne możliwości

8. Zaznajomienie z zakresem odpowiedzialności za ochronę danych osobowych, przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym pozyskaniem lub ujawnieniem.

Szkolenie planuje się przeprowadzić w czasie (łącznie) 2 godzin lekcyjnych (po 45 min) w terminie wyznaczonym przez kierowników poszczególnych wydziałów, oddzielnie dla każdego wydziału, w którym są przetwarzane dane osobowe.

STAROSTA
Witold Borkowski

Załącznik nr 1
do zarządzenia Starosty Lęborskiego z dnia 28 lipca 1999 r.
w sprawie zarządzania bezpieczeństwem zbiorów
danych osobowych oraz ochrony tychże danych
przetwarzanych w Starostwie Powiatowym w Lęborku

INSTRUKCJA
ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH.

§ 1

1. Przydział identyfikatorów i haseł dla osób zatrudnionych przy przetwarzaniu danych osobowych w systemach komputerowych odbywa się zgodnie z wymogami programu komputerowego, który jest wykorzystywany do przetwarzania danych osobowych.
2. Odpowiedzialnymi za przydział haseł dla osób zatrudnionych przy przetwarzaniu danych osobowych w systemach komputerowych przetwarzających dane osobowe są kierownicy wydziałów - dla pracowników swojego wydziału.
3. Hasło użytkownika powinno być zmieniane co najmniej raz na miesiąc.
4. Identyfikator użytkownika przyznaje administrator danych i odnotowuje ten fakt w rejestrze ewidencji osób zatrudnionych przy przetwarzaniu danych.
5. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielany innej osobie.
6. Osobą prowadzącą ewidencję użytkowników zbiorów danych osobowych jest z upoważnienia administratora danych - administrator bezpieczeństwa danych. Rejestr użytkowników wraz z przypisanymi im identyfikatorami administrator bezpieczeństwa danych przechowuje w sposób uniemożliwiający jego zagubienie, kradzież bądź dostęp do niego osób nieuprawnionych.
7. Hasła użytkowników, umożliwiające dostęp do danych osobowych, utrzymuje się w tajemnicy również po upływie ich ważności.

§ 2

1. Procedury rozpoczęcia i zakończenia pracy przy przetwarzaniu danych osobowych określa kierownik wydziału - w zakresie swojej odpowiedzialności.
2. Szczegółowy sposób zarządzania systemem informatycznym służącym do przetwarzania danych, wynikający ze specyfikacji baz danych określa kierownik wydziału.

§ 3

Kopie awaryjne zbiorów informatycznych, w których zawarte są dane osobowe sporządza się w następujący sposób:
1. Po zakończeniu przetwarzania danych w danym dniu pracy sporządza się kopię zbiorów informatycznych na przeznaczonym do tego celu komputerze pracującym w sieci lokalnej. Przed sporządzeniem tej kopii - w miarę potrzeb - dokonuje się indeksakcji zbiorów lub ich sprawdzenia w inny sposób, zgodny z programem, który jest używany do przetwarzania danych osobowych.
2. W każdy piątek - po zakończeniu przetwarzania danych - dokonuje się zapisu kopii awaryjnych zbioru informatycznego na niezależnych nośnikach danych (dyskietki, CD-ROM, dyskietki lub taśmy urządzeń kopiujących). Nośniki te przechowuje się pod zamknięciem, w pomieszczeniu oddzielonym od tych pomieszczeń, w których przechowywane są zbiory danych eksploatowane na bieżąco.
3. Niezależne nośniki danych nie mogą być udostępniane osobom niepowołanym.
4. Odpowiedzialnym za sporządzanie kopii zapasowych zbiorów informatycznych jest kierownik wydziału, który może upoważnić do wykonywania tych czynności pracownika wydziału.

§ 4

Administrator bezpieczeństwa danych przynajmniej raz w miesiącu dokonuje sprawdzenia komputerów, w których są przetwarzane dane osobowe pod kątem obecności wirusów dostępnymi na rynku (przynajmniej dwoma) programami antywirusowymi. Z dokonanego sprawdzenia pozostawia na danym komputerze zapis w postaci pliku informacyjnego, zabezpieczonego przed otwarciem przez inne osoby.

W przypadku zawirusowania komputera ustala się najbardziej bezpieczny (wynikający z charakteru i typu wirusa) sposób jego usunięcia.
W przypadku konieczności naprawy nośnika danych po jego zawirusowaniu przez specjalistyczne zakłady naprawcze, usuwa się dane z nośnika w sposób uniemożliwiający ich odczytanie za pomocą standardowych komend systemu operacyjnego komputera. Odpowiedzialnym za całkowite i nie do odzyskania usunięcie danych w takim przypadku jest administrator bezpieczeństwa danych.

§ 5

1. Udostępnianie danych osobowych, a w szczególności sporządzanie wydruków tych danych może nastąpić na rzecz osób lub podmiotów:
   a) uprawnionych do ich otrzymania na mocy przepisów prawa,
   b) które w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw osób, których dane dotyczą.
2. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis szczególny stanowi inaczej.
3. Udostępnienie danych osobowych, w szczególności sporządzanie wydruków może nastąpić tylko przez osoby dopuszczone do przetwarzania danych osobowych przez administratora danych.
4. Pomieszczenia lub części pomieszczeń, w których znajdują się informatyczne bazy danych muszą być oddzielone od miejsc przyjmowania interesantów a sposób udostępniania danych, ustawienie komputerów i drukarek muszą uniemożliwiać wgląd do danych osobom nieuprawnionym.
5. Brudnopisy wydruków wykonane na podstawie informacji ze zbiorów danych osobowych muszą być - przed ich wyrzuceniem - pozbawione możliwości odczytu przez osoby nieuprawnione - np. przez pocięcie na niszczarce.

§ 6

1. Komputer, na którym są przechowywane i przetwarzane dane osobowe nie może być podłączony do informatycznej sieci zewnętrznej.
2. Dostęp do komputera, na którym są przetwarzane dane osobowe może być utworzony tylko dla osób dopuszczonych przez administratora danych do prac nad przetwarzaniem danych osobowych, w zakresie i stopniu niezbędnym do wykonywania przez te osoby obowiązków służbowych.
3. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.

§ 7

1. Łączność przy wykorzystaniu komputerów, na których odbywa się przetwarzanie danych osobowych, może odbywać się tylko w ramach sieci lokalnej.
2. W przypadku konieczności stosowania łączności zewnętrznej - na czas trwania tej łączności odłącza się komputer z sieci lokalnej i pozostaje on w tym stanie do czasu zakończenia łączności i wyłączenia modemu.
3. Komputer mający dostęp do informatycznej sieci zewnętrznej nie może mieć połączenia z komputerami pracującymi w sieci lokalnej. Komputer ten nie może być ponadto wykorzystywany do przetwarzania danych osobowych.
4. Odpowiedzialnym za organizację łączności zewnętrznej jest administrator bezpieczeństwa danych.

§ 8

1. W przypadku konieczności likwidacji nośnika danych pozbawia się te nośniki możliwości odczytu danych przez usunięcie zbiorów w sposób uniemożliwiający ich odczytanie lub fizyczne zniszczenie nośników.
2. W przypadku konieczności naprawy nośnika danych, pozbawia się przed naprawą możliwości odczytu danych osobowych albo naprawia się je pod nadzorem administratora bezpieczeństwa danych.

§ 9

1. Osoba dopuszczona przez administratora danych do przetwarzania danych osobowych ma obowiązek:
   a) utrzymania w tajemnicy danych osobowych osób zarejestrowanych w zasobach informatycznych,
   b) dołożenia wszelkich starań w zakresie ochrony danych osobowych przed dostępem ze strony osób nieuprawnionych,
   c) informowania przełożonych oraz administratora bezpieczeństwa danych o wszelkich nieprawidłowościach w działaniu informatycznej bazy danych, szczególnie mogących świadczyć o naruszeniu bezpieczeństwa tych danych,
2. Obowiązek zachowania tajemnicy przez osobę zatrudnioną przy przetwarzaniu danych osobowych istnieje również po ustaniu zatrudnienia.

STAROSTA
Witold [illegible]kowski

Załącznik nr 3
do zarządzenia Starosty Lęborskiego z dnia 29 lipca 1999 r.
w sprawie zarządzania bezpieczeństwem zbiorów
danych osobowych oraz ochrony tychże danych
przetwarzanych w Starostwie Powiatowym w Lęborku

INSTRUKCJA
POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH
DLA OSÓB ZATRUDNIONYCH PRZY PRZETWARZANIU TYCH DANYCH.

§ 1

1. Niniejsza instrukcja określa tryb postępowania w przypadku, gdy:
   a) stwierdzono naruszenie zabezpieczenia systemu informatycznego,
   b) stwierdzono naruszenie zabezpieczenia zbiorów prowadzonych w formie tradycyjnej
   c) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych,
   d) stan pomieszczenia, szaf, biurek, jak również zawartość zbioru danych osobowych mogą wskazywać na naruszenie zabezpieczeń tych danych
2. Niniejsza instrukcja dotyczy wszystkich osób zatrudnionych przy przetwarzaniu danych osobowych
3. Przez system informatyczny należy rozumieć system przetwarzania informacji wraz ze związanymi z nim ludźmi oraz zasobami technicznymi i finansowymi, który dostarcza i rozprowadza informacje.
4. Przez zabezpieczenie systemu informatycznego oraz zbiorów danych osobowych prowadzonych w formie tradycyjnej należy rozumieć wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą.

§ 2

1. Naruszenie zabezpieczenia systemu informatycznego oraz zabezpieczenie zbiorów tradycyjnych w warunkach Starostwa Lęborskiego może nastąpić poprzez:
   a) umożliwienie dostępu do bazy danych zawierającej dane osobowe osobom nieuprawnionym bądź nieuprawnionym i dokonywanie przez nich operacji polegających na zapoznaniu się ze zbiorem, modyfikacji zbioru, kopiowaniu zbioru lub jego części, zniszczeniu zbioru lub jego części,
   b) kradzież nośnika zbioru danych osobowych lub nośnika, na którym zapisano kopie awaryjne, kradzież kartotek, skorowidzów, ksiąg, wykazów i innych zbiorów ewidencyjnych
   c) przekazanie zbioru danych osobowych lub jego części osobom nieuprawnionym bądź nieupoważnionym przez osoby zatrudnione przy przetwarzaniu danych,
   d) dostęp osób nieuprawnionych bądź nieupoważnionych do wydruków, brudnopisów wydruków i innej dokumentacji opracowanej na podstawie zbioru danych osobowych,
   e) zniszczenie bądź modyfikacja zbioru danych osobowych wywołana działaniem wirusa komputerowego bądź niedbałą lub niefachową obsługą systemów komputerowych przez osoby zatrudnione przy przetwarzaniu danych osobowych jak również zniszczenie bądź modyfikacja zbioru danych osobowych prowadzonych w formie tradycyjnej wywołane zdarzeniami losowymi
2. W przypadku naruszenia ochrony danych osobowych w systemie informatycznym objawami tego stanu rzeczy będą:
   a) brak nośnika danych ze zbiorami (lub brak nośników z kopią awaryjną),
   b) niezgodność danych zawartych w systemie komputerowym z dokumentacją tradycyjną,
   c) brak w zbiorze części danych osobowych, brak całego zbioru albo brak plików, w których są zapisywane dane osobowe,
   d) niemożność otwarcia zbioru i korzystania z niego,
   e) brak zgodności atrybutów pliku, w którym zawarte są dane osobowe z atrybutami pozostałymi po wykonaniu na nim operacji przez osoby uprawnione
3. W przypadku naruszenia bezpieczeństwa danych osobowych prowadzonych w sposób tradycyjny objawami tego będą:
   a) brak zbioru danych osobowych,
   b) zerwane plomby pomieszczeń lub sejfów, otwarte pomieszczenia, szafy, biurka itp.,
   c) inne ślady świadczące o dotarciu do zbioru danych osobowych przez osoby postronne.

§ 3

Każdy pracownik zatrudniony przy przetwarzaniu danych osobowych przed rozpoczęciem właściwej pracy ma obowiązek sprawdzić stan zabezpieczenia pomieszczeń, stan zamknięć sejfów, szaf, biurek i innych miejsc, gdzie są przechowywane zbiory danych osobowych prowadzone w sposób tradycyjny i za pomocą systemów informatycznych.

§ 4

1. W przypadku stwierdzenia naruszenia zabezpieczenia zbioru danych osobowych, każda osoba ma obowiązek:
   a) niezwłocznie powiadomić o powyższym kierownika wydziału oraz administratora bezpieczeństwa informacji,
   b) zaprzestać wykonywania operacji na zbiorze danych, w którym zaistniało zdarzenie mogące wskazywać na naruszenie zabezpieczeń tych danych.
2. Po otrzymaniu informacji o możliwości naruszenia zabezpieczenia danych osobowych, administrator bezpieczeństwa danych - wspólnie z kierownikiem wydziału i osobami zatrudnionymi przy przetwarzaniu danych osobowych - ma obowiązek:
   a) zabezpieczyć wszelkie ślady włamania lub kradzieży do dalszych czynności
   b) ustalić faktyczny zakres naruszenia bezpieczeństwa danych, przyczynę i sposób jego dokonania oraz skutki wynikające z naruszenia bezpieczeństwa,
   c) zminimalizować szkody wynikające z naruszenia bezpieczeństwa danych,
   d) w przypadku systemu informatycznego:
      - dokonać kontroli i weryfikacji istniejących zabezpieczeń systemu informatycznego,
      - dokonać sprawdzenia systemu komputerowego pod kątem jego zawirusowania bądź ustalenia innych przyczyn mogących powodować brak bezpieczeństwa danych osobowych,
      - odtworzyć dane z kopii awaryjnej,
      - wezwać osobę upoważnioną przez administratora danych do obsługi systemu informatycznego.
   e) w przypadku zbioru danych prowadzonych w formie tradycyjnej:
      - dokonać kontroli i weryfikacji istnienia zabezpieczeń,
      - uzupełnić, uaktualnić bądź sprostować naruszony zbiór danych osobowych,
      - w przypadku kradzieży - odtworzyć brakujący zbiór danych osobowych.

§ 5

Administrator bezpieczeństwa danych z każdej sytuacji, gdzie stwierdzono naruszenie zabezpieczenia systemu informatycznego sporządza pisemny protokół, który powinien zawierać:
   a) imię i nazwisko osoby, która stwierdziła naruszenie zabezpieczenia danych osobowych,
   b) wskazanie ewentualnej przyczyny naruszenia zabezpieczenia danych osobowych i opis zaistniałej sytuacji,
   c) wskazanie osoby odpowiedzialnej za bezpieczeństwo danych i, o ile to możliwe, osoby podejrzanej o naruszenie bezpieczeństwa danych osobowych,
   d) ustalenia dotyczące naruszonych zasobów (jakie naruszono zabezpieczenia i w jakim stanie zastano nośniki informacji, tradycyjne zbiory,
   e) ewentualne propozycje lepszego zabezpieczenia zbiorów w przyszłości.

§ 6

Z niniejszą instrukcją zapoznać należy wszystkie osoby zatrudnione przy przetwarzaniu danych osobowych. Osoby te fakt zapoznania z instrukcją potwierdzają w formie podpisu na specjalnie do tego celu sporządzonym wykazie.

STAROSTA

Witold Bańkowski