ZARZĄDZENIE Nr 116/2004
Burmistrza Miasta Pułtuska
z dnia 1 grudnia 2004 roku

w sprawie ochrony danych osobowych w Urzędzie Miejskim w Pułtusku

Na podstawie art. 31 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (Dz. U. z 2001r. Nr 142, poz. 1591 z późn. zm.) oraz art. 36 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.) i 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 (Dz. U. z 2004r. Nr 100, poz. 1024):

§1

1. Wprowadza się instrukcję określającą sposób zarządzania systemem informatycznym w Urzędzie Miejskim w Pułtusku - stanowiącą załącznik nr 1 do Zarządzenia.
2. Wprowadza się instrukcję określającą sposób postępowania w przypadku naruszenia bezpieczeństwa danych osobowych i systemów informatycznych je przetwarzających - stanowiącą załącznik nr 2 do Zarządzenia.

§2

Traci moc Zarządzenie Burmistrza Nr 1/99 z dnia 12.02.1999r. w sprawie zasad przetwarzania danych osobowych i technicznych warunków zabezpieczenia systemów informatycznych zawierających te dane.

§3

Zarządzenie wchodzi w życie z dniem podjęcia.

Burmistrz Miasta Pułtusk
(-) mgr inż. Wojciech Dębski

Załącznik Nr 1
do Zarządzenia Nr 116/2004
Burmistrza Miasta Pułtusk
z dnia 1 grudnia 2004 r.

INSTRUKCJA określająca sposób zarządzania systemem informatycznym w Urzędzie Miejskim w Pułtusku.

1. Za bezpieczeństwo danych osobowych w systemie informatycznym odpowiedzialny jest administrator bezpieczeństwa informacji.
2. Administrator bezpieczeństwa informacji prowadzi rejestr systemu informatycznego, w którym odnotowuje wszystkie fakty dotyczące informacji w systemie.
3. System informatyczny pracuje w sieci lokalnej.
   Do pracy w sieci każdy użytkownik musi posiadać unikalny identyfikator i hasło nadane przez Administratora bezpieczeństwa informacji. W sieci mogą pracować jedynie osoby upoważnione. Inne osoby mogą towarzyszyć pracownikom upoważnionym do pracy na zbiorach osobowych tylko za zgodą administratora danych.
4. Rejestrowanie nowych użytkowników musi być poprzedzone szkoleniem w zakresie ochrony danych osobowych. Rejestracja jest związana z przydzieleniem użytkownikowi indywidualnej nazwy (identyfikator), hasła, praw dostępu do danych.
   Zarejestrowanie nowego użytkownika musi być odnotowane w Rejestrze systemu (Nazwisko, imię nazwa użytkownika, prawa dostępu do danych osobowych, data rejestracji, własnoręczny podpis).
5. Wyrejestrowanie użytkownika odbywa się niezwłocznie po utracie jego uprawnień do przetwarzania danych osobowych. Wyrejestrowanie użytkownika musi być odnotowane w Rejestrze systemu (Nazwisko, imię, nazwa użytkownika, aktualne prawa dostępu, data wyrejestrowania, własnoręczny podpis).
6. Rejestrację lub wyrejestrowanie użytkownika przeprowadza Administrator bezpieczeństwa informacji albo inna osoba wskazana przez Administratora danych.
7. System udostępnia dane wyłącznie upoważnionym osobom po podaniu identyfikatora i właściwego hasła.
8. Hasła użytkowników zmieniane są co miesiąc (w pierwszym tygodniu miesiąca).
9. Hasła użytkownika utrzymuje się w tajemnicy, również po upływie ich ważności.

10. Identyfikator użytkownika jest niezmienny, a po wyrejestrowaniu użytkownika nie może być przydzielony innym osobom.
11. Czas pracy przy przetwarzaniu zbiorów danych osobowych pokrywa się z czasem pracy urzędu (w poniedziałek 8.00 – 17.00, a w pozostałe dni 8.00 – 16.00).
    Praca przy przetwarzaniu zbiorów poza tymi godzinami wymaga zgody Administratora danych. Fakt taki powinien być każdorazowo odnotowany w Rejestrze systemu. W trakcie przerw w przetwarzaniu danych użytkownicy muszą przerwać pracę w systemie i uniemożliwić innym osobom dostęp do danych osobowych.
12. Stanowiska pracy powinny być tak zorganizowane , aby uniemożliwić wgląd lub dostęp do danych osobowych przez osoby nieupoważnione.
13. Kopie awaryjne tworzone są po zakończeniu pracy, nie rzadziej niż raz w tygodniu. Częstotliwość tworzenia kopii wynika z czasu dokonywania zmian w zbiorach danych. Kopie awaryjne tworzone są przy użyciu zewnętrznych nośników magnetycznych. Kopie tworzone są na przemian na jednym z dwóch dysków zewnętrznych. Fakt wykonania archiwum odnotowuje się w Rejestrze systemu. Zapis taki powinien zawierać: nazwę archiwum, czas utworzenia, zakres danych, i osobę wykonującą archiwum. Kopie awaryjne należy sprawdzać pod kątem dalszej przydatności przynajmniej raz w miesiącu. Po okresie przydatności należy je bezzwłocznie usunąć w sposób uniemożliwiający ich odtworzenie.
14. Przed wykonaniem archiwum należy sprawdzić system pod kątem występowania wirusów przy wykorzystaniu specjalistycznego oprogramowania. W przypadku wykrycia wirusa należy podjąć próbę jego bezpiecznego usunięcia. Do usuwania należy wykorzystać odpowiednie oprogramowanie zapewniające bezpieczne usunięcie. Po usunięciu należy sprawdzić poprawność danych osobowych oraz ustalić sposób infekcji. W przypadku podejrzenia o uszkodzenie zbioru danych osobowych należy go odtworzyć z ostatniej kopii bezpieczeństwa. O takim fakcie należy powiadomić Administratora danych i zarejestrować ten fakt w Rejestrze Systemu.
15. Kopie i wydruki archiwalne przechowywane są w archiwum Urzędu.
16. Przeglądy systemu dokonywane są okresowo przynajmniej raz w tygodniu. W trakcie przeglądu analizowane są zbiory plików rejestrowych, odtwarzane (w razie konieczności) zbiory indeksów, wyszukiwane wirusy komputerowe, poszukiwanie zbiorów na dysku.
17. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.

18. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych, pozbawia się wcześniej zapisu tych danych.
19. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się wcześniej zapisu tych danych albo naprawia się pod nadzorem Administratora bezpieczeństwa informacji.
20. Przy przekazaniu danych osobowych konieczne jest zachowanie szczególnej ostrożności.
21. Rejestr wniosków o udostępnienie informacji ze zbioru danych osobowych prowadzony jest w każdym Wydziale przetwarzającym dane osobowe.
22. wzór wykazu osób, które zapoznały się z „Instrukcją określającą sposób zarządzania systemem informatycznym w Urzędzie Miejskim w Pułtusku" stanowi Załącznik Nr 1 do niniejszej instrukcji.
23. Wzór oświadczenia o zapoznaniu się z przepisami dotyczącymi tajemnicy służbowej, zasadach przetwarzania i zabezpieczenia danych osobowych, oraz o odpowiedzialności karnej za naruszenie ochrony danych osobowych stanowi Załącznik Nr 2 do niniejszej instrukcji.

Załącznik Nr 1 do „Instrukcji określającej sposób zarządzania systemem informatycznym w Urzędzie Miejskim w Pułtusku”

Wykaz osób,
które zostały zapoznane z „Instrukcją określającą sposób zarządzania systemem informatycznym w Urzędzie Miejskim w Pułtusku”,
przeznaczona dla osób zatrudnionych przy przetwarzaniu danych osobowych.

Lp.	Nazwisko i imię	Stanowisko	Data	Podpis

Załącznik Nr 2 do „Instrukcji określającej sposób zarządzania systemem informatycznym w Urzędzie Miejskim w Pułtusku”

…….. Pułtusk, dn. ……..
(imię i nazwisko pracownika)

……..
(adres)
……..

OŚWIADCZENIE

(tekst oświadczenia podpisanego przez pracowników Urzędu Miejskiego w Pułtusku)

1. Stwierdzam własnoręcznym podpisem, że znana mi jest treść przepisów:
   a) o ochronie i postępowaniu z wiadomościami, stanowiącymi tajemnicę służbową - ustawa z dnia 22 stycznia 1999r. o ochronie informacji niejawnych (Dz. U. z 1999r. Nr 11 poz. 95 z późn. zm.)
   b) o zasadach przetwarzania i zabezpieczenia danych osobowych, oraz o odpowiedzialności karnej za naruszenie ochrony danych osobowych - ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.) i rozporządzenie 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 (Dz. U. z 2004r. Nr 100, poz. 1024).
2. Jednocześnie zobowiązuję się nie ujawniać wiadomości, z którymi zapoznałem/zapoznałam się z racji wykonywanej pracy w Urzędzie Miejskim, a w szczególności nie będę:
   a) ujawniać danych zawartych w eksploatowanych w Urzędzie systemach informatycznych, zwłaszcza danych osobowych znajdujących się w tym systemach,
   b) ujawniać szczegółów technologicznych używanych w Urzędzie systemów oraz oprogramowania,
   c) udostępniać osobom nieupoważnionym nośniki magnetyczne i optyczne oraz wydruki komputerowe,
   d) kopiować lub przetwarzać danych w sposób inny niż dopuszczony obowiązującą instrukcją technologiczną.

…….. ……
(podpis pracownika) (podpis przełożonego)

Załącznik Nr 2
do Zarządzenia Nr 116/2004
Burmistrza Miasta Pułtusk
z dnia 1 grudnia 2004 r.

INSTRUKCJA określająca sposób postępowania
w przypadku naruszenia ochrony danych osobowych i systemów informatycznych je przetwarzających

1. W przypadku stwierdzenia naruszenia zabezpieczeń systemu informatycznego, gdy 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, każdy pracownik zobowiązany jest do:
   a) zabezpieczenia miejsca zdarzenia w sposób uniemożliwiający dalsze korzystanie ze zbiorów danych osobowych oraz zmianę stanu faktycznego,
   b) niezwłocznego powiadomienia Administratora bezpieczeństwa informacji,
   c) oczekiwania w miejscu zdarzenia na Administratora bezpieczeństwa informacji lub inną osobę upoważnioną przez Administratora danych,
   d) udzielenia wyjaśnień dotyczących zdarzenia
2. Administrator bezpieczeństwa informacji lub inna osoba wskazana przez administratora danych zabezpiecza miejsce zdarzenia w celu zabezpieczenia danych osobowych jak również dowodów mających wpływ na określenie zakresu naruszenia ochrony danych. Administrator bezpieczeństwa informacji sporządza raport stwierdzający naruszenie zabezpieczeń systemu informatycznego w Urzędzie Miejskim w Pułtusku, którego wzór stanowi Załącznik Nr 1 do niniejszej instrukcji, a następnie przekazuje go Administratorowi danych.
3. W razie konieczności wyjaśnienia faktów określonych w pkt. 1 Administrator danych powołuje komisję, w skład której wchodzi Administrator bezpieczeństwa informacji, Sekretarz Miasta Pułtusk oraz osoba posiadająca ogólną wiedzę z zakresu przetwarzania danych.
4. Komisja ma na celu ustalenie:
   1) czy doszło do naruszenia danych osobowych,
   2) jeżeli doszło do naruszenia danych, należy określić jego stopień,
   3) ustalenie osoby odpowiedzialnej za uchybienia,
   4) ustalenie środków zapobiegawczych i naprawczych.
5. Ustalenie komisji w formie protokołu przekazywane są do Administratora danych.

Załącznik Nr 1 do „Instrukcji określającej sposób postępowania w przypadku naruszenia danych osobowych”

Raport

stwierdzający naruszenie zabezpieczeń systemu informatycznego w Urzędzie Miejskim w Pułtusku

1. Data: …… Godzina: ……
(dd.mm.rr) (gg:mm)

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

……..
(imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje)

3. Lokalizacja zdarzenia:

……..
(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:
……..
……..
……..

5. Przyczyny wystąpienia zdarzenia:
……..
……..
……..

6. Podjęte działania:
……..
……..
……..

7. Postępowanie wyjaśniające:
……..
……..
……..

……..
(data, podpis Administratora Bezpieczeństwa Informacji)