Załącznik Nr 1
do Zarządzenia Nr 13/06
Starosty Gostyńskiego
z dnia 28 lutego 2006 r.

„Polityka bezpieczeństwa systemów informatycznych”
służących do przetwarzania danych osobowych
w Starostwie Powiatowym w Gostyniu

Opracował: Administrator Bezpieczeństwa Informacji

Gostyń, luty 2006 r.

SPIS TREŚCI:

WPROWADZENIE

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych w Starostwie Powiatowym w Gostyniu z wyłączeniem Systemów **„POJAZD”** i **„KIEROWCA”** użytkowanych w Wydziale Komunikacji, dla których „Instrukcje bezpieczeństwa” zostały opracowane przez PWPW w Warszawie (administratora systemu).

Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę Urzędu. Dokument zwraca uwagę na konsekwencje jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

Odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi współczesnym systemom informatycznym.

Dokument „Polityka bezpieczeństwa systemów informatycznych” służących do przetwarzania danych osobowych w Urzędzie, zwany dalej „Polityką bezpieczeństwa", wskazuje sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w systemach informatycznych i przeznaczony jest dla osób zatrudnionych przy przetwarzaniu tych danych.

Potrzeba jego opracowania wynika z § 3 i 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. 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. Nr 100, poz. 1024).

„Polityka bezpieczeństwa" określa tryb postępowania w przypadku, gdy:

1) stwierdzono naruszenie zabezpieczenia systemu informatycznego,
2) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci informatycznej mogą wskazywać na naruszenie zabezpieczeń tych danych.

„Polityka bezpieczeństwa" obowiązuje wszystkich pracowników Starostwa Powiatowego w Gostyniu.

Realizacja postanowień tego dokumentu ma zapewnić ochronę danych osobowych, właściwą ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemach informatycznym Urzędu.

1. Administrator danych, którym jest Starosta Gostyński, wyznacza Administratora Bezpieczeństwa Informacji oraz osobę upoważnioną do zastępowania Administratora.
2. Administrator Bezpieczeństwa Informacji realizuje zadania w zakresie ochrony danych, a w szczególności:

1) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Urzędu,
2) podejmowania stosownych działań w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych,
3) niezwłocznego informowania Administratora danych (Starosty) lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
4) nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych,
5) fizycznego zabezpieczenia danych osobowych oraz obiektów, w których są gromadzone i przetwarzane.

3. Osoba zastępująca Administratora Bezpieczeństwa Informacji powyższe zadania realizuje w przypadku nieobecności Administratora Bezpieczeństwa.
4. Osoba zastępująca składa Administratorowi Bezpieczeństwa relację z podejmowanych działań w czasie jego zastępstwa.

„Polityka bezpieczeństwa systemów informatycznych" jest zgodna z następującymi aktami prawnymi:

1) ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.),
2) rozporządzeniem 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. Nr 100, poz. 1024).

Rozdział 1
OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

1. Podział zagrożeń:
   1) Zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu) - ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu; ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych.
   2) Zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania, pogorszenie jakości sprzętu i oprogramowania) - może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.
   3) Zagrożenia zamierzone - świadome i celowe działania powodujące naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na:

- nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
- nieuprawniony dostęp do systemu z jego wnętrza,
- nieuprawnione przekazanie danych,
- bezpośrednie zagrożenie materialnych składników systemu (np. kradzież sprzętu).

2. Naruszenie lub podejrzenie naruszenia systemu informatycznego, w którym przetwarzane są dane osobowe następuje w sytuacji:
   1) losowego lub nieprzewidzianego oddziaływania czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, itp.,
   2) niewłaściwych parametrów środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
   3) awarii sprzętu lub oprogramowania, które wyraźnie wskazuje na umyślne działanie w kierunku naruszenia ochrony danych,
   4) pojawienia się odpowiedniego komunikatu alarmowego,
   5) podejrzenia nieuprawnionej modyfikacji danych w systemie lub innego odstępstwa od stanu oczekiwanego,
   6) naruszenia lub próby naruszenia integralności systemu lub bazy danych w tym systemie,
   7) pracy w systemie wykazującej odstępstwa uzasadniające podejrzenie przełamania lub zaniechania ochrony danych osobowych - np. praca osoby, która nie jest formalnie dopuszczona do obsługi systemu,
   8) ujawnienia nieautoryzowanych kont dostępu do systemu,
   9) naruszenia dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (np. nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, itp.).
3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia fizycznego miejsc przechowywania i przetwarzania danych osobowych np.
   - niezabezpieczone pomieszczenia,
   - nienadzorowane, otwarte szafy, biurka, regały,
   - niezabezpieczone urządzenia archiwizujące,
   - pozostawianie danych w nieodpowiednich miejscach – kosze, stoły itp.

Rozdział 2
ZABEZPIECZENIE DANYCH OSOBOWYCH

1. Administratorem danych osobowych zawartych i przetwarzanych w systemach informatycznych Urzędu jest Starosta Gostyński.

2. Administrator danych osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych Urzędu, a w szczególności:
   1) zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym,
   2) zapobiega przed pobraniem danych przez osobę nieuprawnioną,
   3) zapobiega zmianie, utracie, uszkodzeniu lub zniszczeniu danych,
   4) zapewnia przetwarzanie danych zgodnie z obowiązującymi przepisami prawa.
3. Zadania określone w pkt 2 wykonuje w imieniu Administratora danych osobowych Administrator Bezpieczeństwa Informacji.
4. Techniczną ochronę danych i ich przetwarzania realizuje się poprzez:
   1) przetwarzanie danych osobowych w wydzielonych pomieszczeniach położonych w strefie administracyjnej,
   2) zabezpieczenie pomieszczeń, o których mowa w pkt 1, przed nieuprawnionym dostępem, ze szczególnym uwzględnieniem pomieszczenia serwerowni,
   3) wyposażenie pomieszczeń dające gwarancję bezpieczeństwa dokumentacji (szafy, biurka, itp. zamykane na klucz).
5. Organizacyjną ochronę danych i ich przetwarzania realizuje się poprzez:
   1) zapoznanie każdej osoby z przepisami dotyczącymi ochrony osobowych, przed dopuszczeniem jej do pracy przy ich przetwarzaniu,
   2) przeszkolenie osób, o których mowa w pkt 1, w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych oraz zabezpieczenia pomieszczeń i budynków,
   3) kontrolowanie pomieszczeń, w których są przetwarzane dane osobowe.
6. Niezależnie od niniejszych ustaleń mają zastosowanie wszelkie inne regulaminy i instrukcje dotyczące bezpieczeństwa.
7. Wykaz pomieszczeń, w których przetwarzane są dane osobowe oraz opis systemów informatycznych i ich zabezpieczeń zawiera załącznik nr 1 do niniejszego dokumentu.

Rozdział 3
KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Administrator Bezpieczeństwa Informacji sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikający z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.
2. Administrator Bezpieczeństwa Informacji sporządza roczne plany kontroli zatwierdzone przez Starostę i zgodnie z nimi przeprowadza kontrole oraz dokonuje kwartalnych ocen stanu bezpieczeństwa danych osobowych.

3. Na podstawie zgromadzonych materiałów, o których mowa w pkt 2, Administrator Bezpieczeństwa Informacji sporządza roczne sprawozdanie i przedstawia Staroście.

Rozdział 4
POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. W przypadku stwierdzenia naruszenia:
   1) zabezpieczenia systemu informatycznego,
   2) technicznego stanu urządzeń,
   3) zawartości zbioru danych osobowych,
   4) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
   5) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, kradzież itp.)

   każda osoba jest zobowiązana do niezwłocznego powiadomienia o tym fakcie Administratora Bezpieczeństwa Informacji i bezpośredniego przełożonego.
2. Po wykonaniu czynności określonych w pkt 1 należy:
   1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
   2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
   3) zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę zdarzenia,
   4) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego lub aplikacji użytkowej,
   5) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
   6) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa Informacji lub osoby upoważnionej.
3. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Administrator Bezpieczeństwa Informacji lub osoba go zastępująca:
   1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Urzędu,
   2) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
   3) w razie potrzeby powiadamia o zaistniałym naruszeniu Starostę,

4) jeżeli zachodzi taka potrzeba zleca usuniecie występujących naruszeń, oraz powiadamia odpowiednie instytucje,

4. Administrator Bezpieczeństwa Informacji dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego załącznik nr 2.
5. Raport, o którym mowa w ust. 6, Administrator Bezpieczeństwa Informacji niezwłocznie przekazuje Administratorowi danych osobowych (Staroście), a w przypadku jego nieobecności osobie uprawnionej.
6. Zaistniałe naruszenie może stać się przedmiotem szczegółowej analizy prowadzonej przez zespół powołany przez Starostę.
7. Analiza, o której mowa w pkt 6, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

Rozdział 5
POSTANOWIENIA KOŃCOWE

1. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, wszczyna się postępowanie dyscyplinarne.
2. Administrator Bezpieczeństwa zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych wg wzoru stanowiącego załącznik nr 3 do niniejszego dokumentu.

Załącznik nr 1
do Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Starostwie Powiatowym w Gostyniu.

Wykaz pomieszczeń,
w których przetwarzane są dane osobowe w Starostwie i ich zabezpieczeń.

1. Wykaz pomieszczeń, w których przetwarzane są dane osobowe.

Lp.	Nazwa komórki	Lokalizacja	Nr pokoju
1			

2. W celu ochrony przed utratą danych w Urzędzie stosowane są następujące zabezpieczenia:

1) odrębne zasilanie sprzętu komputerowego oraz zastosowanie zasilaczy awaryjnych UPS,

2) ochrona serwerów przed zanikiem zasilania poprzez stosowanie zasilaczy awaryjnych UPS,

3) ochrona przed utratą zgromadzonych danych przez robienie kopii zapasowych na płytach CD,CDRW, z których w przypadku awarii odtwarzane są dane.

3. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu:

1) aby uzyskać dostęp do zasobów sieci, należy zwrócić się do Administratora Bezpieczeństwa z odpowiednim wnioskiem w którym podane będą dane nowego użytkownika oraz zasoby jakie ma on mieć udostępnione.

2) w systemie informatycznym Urzędu zastosowano podwójną autoryzację użytkownika. Pierwszej autoryzacji należy dokonać w momencie uzyskania dostępu do serwera Urzędu, podając login użytkownika i hasło; drugiej autoryzacji należy dokonać uruchamiając program użytkowy, podając login użytkownika i hasło; dostęp do wybranej bazy danych Urzędu uzyskuje się dopiero po poprawnym podwójnym zalogowaniu się do systemu informatycznego Urzędu.

4. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu poprzez internet.

W zakresie dostępu z sieci wewnętrznej Urzędu do sieci rozległej Internet zastosowano środki ochrony przed podsłuchiwaniem, penetrowaniem i atakiem z zewnątrz. Zastosowano firewall, który ma za zadanie uwierzytelnianie źródła przychodzących wiadomości oraz filtrowanie pakietów w oparciu o adres IP, numer portu i inne parametry. Ściana ogniowa składa się z bezpiecznego systemu operacyjnego i filtra pakietów. Ruch pakietów, który firewall przepuszcza jest określony przez administratora.

Firewall zapisuje do logu fakt zaistnienia wyjątkowych zdarzeń i śledzi ruch pakietów przechodzących przez nią. Dostęp do sieci jest ustalony indywidualnie dla każdego użytkownika na podstawie wniosku.

Oprócz filtra pakietów (firewall) zastosowano również system wykrywający obecność wirusów w poczcie elektronicznej.

W efekcie zapewnione jest:

1) *zabezpieczenie sieci przed atakiem z zewnątrz poprzez blokowanie wybranych portów,*
2) *filtrowanie pakietów i blokowanie niektórych usług,*
3) *objęcie ochroną antywirusową wszystkich danych ściąganych z internetu na stacjach lokalnych,*
4) *zapisywanie logów połączeń użytkowników z siecią Internet.*

5. Postanowienia końcowe.

1) *do pomieszczeń w których następuje przetwarzanie danych osobowych mają dostęp tylko uprawnione osoby bezpośrednio związane z nadzorem nad serwerami lub aplikacjami,*
2) *zabezpieczenie przed nieuprawnionym dostępem do danych, prowadzone jest przez Administratora Bezpieczeństwa Informacji zgodnie z przyjętymi procedurami nadawania uprawnień do systemu informatycznego,*
3) *osoby mające dostęp do danych powinny posiadać zaświadczenie o przebytym szkoleniu z zakresu ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997r.*
4) *w pomieszczeniach w których znajdują się serwery jest zamontowana klimatyzacja, która zapewnia właściwą temperaturę i wilgotność powietrza dla sprzętu komputerowego*
5) *większość urządzeń w serwerowni umieszczona jest w szafach serwerowych i sieciowych.*

Załącznik nr 2
do Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Starostwie Powiatowym w Gostyniu.

R a p o r t

z naruszenia bezpieczeństwa systemu informatycznego w Starostwie Powiatowym w Gostyniu.

1. Data:.....Godzina:.....
(dd.mm.rrrr) *(00:00)*

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....
(Imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje))

4. Lokalizacja zdarzenia:

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

5. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....

.....

6. Podjęte działania:

.....

.....

7. Przyczyny wystąpienia zdarzenia:

.....

.....

8. Postępowanie wyjaśniające:

.....

.....

.....
data, podpis Administratora Bezpieczeństwa Informacji

Załącznik nr 3
do Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Starostwie Powiatowym w Gostyniu.

Wykaz osób,

które zostały zapoznane z „Polityką bezpieczeństwa systemów informatycznych” służących do przetwarzania danych osobowych w Urzędzie Starostwie Powiatowym.

Przyjąłem/am/ do wiadomości i stosowania zapisy Polityki bezpieczeństwa.

Lp	Nazwisko i imię	Komórka organizacyjna	Data, podpis