Załącznik nr 2
do Zarządzenia nr 13/06
Starosty Gostyńskiego
z dnia 28 lutego 2006 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM STAROSTWA POWIATOWEGO W GOSTYNIU

I. Podstawa prawna.

ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz rozporządzenie 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 z późn. zm.)

II. Przepisy ogólne.

1. Instrukcja zarządzania systemem informatycznym Starostwa Powiatowego w Gostyniu, zwana dalej instrukcją, opisuje sposoby nadawania uprawnień użytkownikom, określa sposób pracy w systemie informatycznym, procedury zarządzania oraz czynności mające wpływ na zapewnienie bezpieczeństwa systemu informatycznego Starostwa Powiatowego w Gostyniu.
2. Niniejsza instrukcja realizuje „Politykę bezpieczeństwa systemu informatycznego" obowiązującą w Starostwie Powiatowym w Gostyniu.

III. Definicje.

1. Ilekroć w niniejszym dokumencie jest mowa o:
a) Urzędzie – należy przez to rozumieć Starostwo Powiatowe w Gostyniu,
b) Administratorze Danych – należy przez to rozumieć Starostę Gostyńskiego,
c) Administratorze Bezpieczeństwa Informacji – należy przez to rozumieć wyznaczonego pracownika do nadzorowania przestrzegania zasad ochrony danych osobowych ustanowionego zgodnie z Polityką bezpieczeństwa przetwarzania danych osobowych Urzędu,
d) Administratorze Systemu Informatycznego – należy przez to rozumieć osobę odpowiedzialną za funkcjonowanie systemu informatycznego Urzędu oraz stosowanie technicznych i organizacyjnych środków ochrony,
e) użytkowniku systemu – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym Urzędu.
f) sieci lokalnej – należy przez to rozumieć połączenie systemów informatycznych Urzędu wyłącznie dla własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych,
g) sieci rozległej – należy przez to rozumieć sieć publiczną w rozumieniu ustawy z dnia 21 lipca 2000r. – Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.)
2. W Starostwie Powiatowym w Gostyniu funkcję Administratora Systemu Informatycznego pełni Administrator Bezpieczeństwa Informacji.

IV. Procedury nadawania i zmiany uprawnień do przetwarzania danych.

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:
   - Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 Nr 101, poz. 926 z późn. zm.),
   - Polityką bezpieczeństwa przetwarzania danych osobowych systemu informatycznego,
   - niniejszym dokumentem,

   oraz posiadać upoważnienie do przetwarzania danych osobowych.
2. Zapoznanie się z powyższymi informacjami pracownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi załącznik nr 1.
3. Administrator Systemu Informatycznego przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnego upoważnienia (wniosku) określającego zakres uprawnień pracownika, którego wzór stanowi załącznik nr 2, z wyłączeniem osób kierujących Starostwem.
4. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora, hasła oraz zakresu dostępnych danych i operacji.
5. Hasło ustanowione podczas przyznawania uprawnień przez Administratora Systemu Informatycznego należy zmienić na indywidualne podczas pierwszego logowania się w systemie.
6. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.
7. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
8. W systemie informatycznym stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do sieci lokalnej oraz dostępu do aplikacji.
9. Identyfikator użytkownika w aplikacji (o ile działanie aplikacji na to pozwala), powinien być tożsamy z tym, jaki jest mu przydzielany w sieci lokalnej.
10. Odebranie uprawnień pracownikowi następuje na pisemny wniosek przełożonego, któremu pracownik podlega z podaniem daty oraz przyczyny odebrania uprawnień.
11. Kierownicy komórek organizacyjnych zobowiązani są pisemnie informować Administratora o każdej zmianie dotyczącej podległych pracowników mającej wpływ na zakres posiadanych uprawnień w systemie informatycznym.
12. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane oraz unieważnić jej hasło.
13. Administrator Systemu Informatycznego zobowiązany jest do prowadzenia i ochrony rejestru użytkowników i ich uprawnień w systemie informatycznym. rejestr stanowi załącznik nr 3,

V. Zasady posługiwania się hasłami.

1. Bezpośredni dostęp do systemu informatycznego może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
2. Hasło użytkownika powinno być zmieniane co najmniej raz w miesiącu.

3. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.
4. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł.
5. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
6. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
7. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła.
8. Przy wyborze hasła obowiązują następujące zasady:
   a) minimalna długość hasła - 6 znaków,
   b) zakazuje się stosować: haseł, które użytkownik stosował uprzednio w okresie minionego roku, swojej nazwy użytkownika w jakiejkolwiek formie (pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę, itp.), swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiejkolwiek formie, imion (w szczególności imion osób z najbliższej rodziny), ogólnie dostępnych informacji o użytkowniku takich jak: numer telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego, nazwa ulicy na której mieszka lub pracuje, itp. wyrazów słownikowych, przewidywalnych sekwencji znaków z klawiatury np.: QWERTY”,”12345678”,itp.
   c) należy stosować:
      - hasła zwierające kombinacje liter i cyfr,
      - hasła zawierające znaki specjalne: znaki interpunkcyjne, nawiasy, symbole @, #, &, itp. o ile system informatyczny na to pozwala,
      - hasła, które można zapamiętać bez zapisywania,
      - hasła łatwe i szybkie do wprowadzenia, po to by trudniej było podejrzeć je osobom trzecim,
9. Zmiany hasła nie wolno zlecać innym osobom.
10. W systemach, które umożliwiają opcję zapamiętania nazw użytkownika lub jego hasła nie należy korzystać z tego ułatwienia.
11. Hasło użytkownika o prawach administratora powinno znajdować się w zalakowanej kopercie w zamykanej na klucz szafie metalowej, do której dostęp mają:
    - Administrator Bezpieczeństwa Informacji,
    - Starosta, Sekretarz lub inna upoważniona osoba.

VI. Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie.

1. Przed rozpoczęciem pracy w systemie komputerowym należy zameldować się do systemu przy użyciu indywidualnego identyfikatora oraz hasła.
2. Przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wykonać opcję wymeldowania z systemu (zablokowania dostępu), lub jeżeli taka możliwość nie istnieje wyjść z programu.
3. Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązana jest wykonać funkcję wymeldowania z systemu.
4. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów, wykonać zamknięcie systemu i jeżeli jest to konieczne wymeldować się z sieci komputerowej

5. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania oraz zakończeniem pracy w sieci.

VII. Procedury tworzenia zabezpieczeń.

A. Za systematyczne przygotowanie kopii bezpieczeństwa odpowiada Administrator Systemu Informatycznego.
B. Kopie bezpieczeństwa wykonywane są codzienne po zakończeniu pracy wszystkich użytkowników w sieci komputerowej.
C. Kopie bezpieczeństwa wykonywane są na płytach CD lub innym nośniku,
   - Każdą płytę wykorzystuje się do zrobienia kopii z trzech dni roboczych.
   - Każdy płytę przechowuje 7 ostatnich kopii.
D. Dodatkowe zabezpieczenie wszystkich programów i danych wykonywane jest w pierwszym dniu każdego miesiąca w postaci zapisu na płytach CD-R, DVD-R lub taśmach magnetycznych
E. W przypadku wykonywania zabezpieczeń długoterminowych na taśmach magnetycznych lub dyskietkach, nośniki te należy co kwartał sprawdzać pod kątem ich dalszej przydatności.

VIII. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz wydruków.

A. Elektroniczne nośniki informacji.
   1. Dane osobowe w postaci elektronicznej - za wyjątkiem kopii bezpieczeństwa – zapisane na dyskietkach, dyskach magnetooptycznych czy dyskach twardych nie są wynoszone poza siedzibę Urzędu.
   2. Wymienne elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych, określony w Polityce bezpieczeństwa przetwarzania danych osobowych.
   3. Po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki informacji są przechowywane w zamykanych szafach biurowych lub kasetkach.
   4. 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.
   5. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymywania danych osobowych pozbawia się wcześniej zapisu tych danych.
   6. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej.

B. Kopie zapasowe.
   1. Kopie bezpieczeństwa są przechowywane w szafie w pokoju 34 w budynku Urzędu.
   2. Dostęp do danych opisanych w punkcie 1 ma Administrator Systemu Informatycznego oraz upoważnieni pracownicy.

C. Wydruki.
   1. W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym.
   2. Pomieszczenie, w którym przechowywane są wydruki robocze musi być należycie zabezpieczone po godzinach pracy.
   3. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

IX. Środki ochrony systemu przed złośliwym oprogramowaniem i wirusami komputerowymi.

1. Na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe pracujące w trybie monitora.
2. Każdy e-mail wpływający do Urzędu musi być sprawdzony pod kątem występowania wirusów przez bramę antywirusową.
3. Definicje wzorców wirusów aktualizowane są nie rzadziej niż raz w miesiącu.
4. Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje użytkownik, który nośnik zamierza użyć.
5. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.
6. Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje pracownik, który pocztę otrzymał.
7. Administrator Systemu Informatycznego przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach - minimum co trzy miesiące.
8. Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania.
9. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe na którym wirusa wykryto oraz wszystkie posiadane przez użytkownika nośniki.

X. Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych.

1. Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie osobom uprawnionym.
2. Udostępnienie danych osobowych nie może być realizowane drogą telefoniczną.
3. Aplikacje wykorzystywane do obsługi baz danych osobowych powinny zapewniać odnotowanie informacji o udzielonych odbiorcom danych. Zakres informacji powinien obejmować co najmniej: dane odbiorcy, datę wydania, zakres udostępnionych danych.

XI. Procedury wykonywania przeglądów i konserwacji systemu.

A. Przeglądy i konserwacja urządzeń.
   1. Przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonym przez producenta sprzętu.
   2. Nieprawidłowości ujawnione w trakcie tych działań powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. O fakcie ujawnienia nieprawidłowości należy zawiadomić Administratora Bezpieczeństwa Informacji.

B. Przegląd programów i narzędzi programowych.
   1. Konserwacja baz danych przeprowadzana jest zgodnie z zaleceniami twórców poszczególnych programów.
   2. Administrator Bezpieczeństwa Informacji zobowiązany jest uaktywnić mechanizm zliczania nieudanych prób zameldowania się do systemu oraz ustawić blokadę konta użytkownika po wykryciu trzech nieudanych prób, we wszystkich systemach posiadających taką funkcję.
   3. Wszystkie logi opisujące pracę systemu, zameldowania i wymeldowania użytkowników oraz rejestr z systemu śledzenia wykonywanych operacji w programie należy przed usunięciem zapisać na płytę CD-R/DVD-R.

C. Rejestracja działań konserwacyjnych, awarii oraz napraw.
   1. Administrator Bezpieczeństwa Informacji prowadzi „Dziennik systemu informatycznego Urzędu Gminy”. Wzór i zakres informacji rejestrowanych w dzienniku określony jest w Załączniku Nr 6.
   2. Wpisów do dziennika może dokonywać Administrator Danych, Administrator Bezpieczeństwa Informacji lub osoby przez nich wyznaczone.

XII. Połączenie do sieci Internet.

Połączenie lokalnej sieci komputerowej Urzędu z Internetem jest dopuszczalne wyłącznie po zainstalowaniu mechanizmów ochronnych (firewal) oraz oprogramowania antywirusowego.

Załącznik nr 1
do Instrukcji Zarządzania
Systemem Informatycznym

Gostyń, dnia .....

.....
(nazwisko i imię)

.....
(nazwa komórki)

.....
(stanowisko)

OŚWIADCZENIE

Oświadczam, iż w związku z przetwarzaniem danych osobowych wynikających z wykonywanych przeze mnie czynności służbowych zapoznałem(am) się z:

1. Ustawą z dnia 29.08.1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z poźn. zm.),
2. Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29.04.2004r. 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).
3. Dokumentem „Polityka bezpieczeństwa systemu informatycznego”.
4. Dokumentem „Instrukcja zarządzania systemem informatycznym”.

.....
(podpis pracownika)

Załącznik nr 2
do Instrukcji Zarządzania
Systemem Informatycznym

WNIOSEK
O NADANIE UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

☐ Nowy użytkownik	☐ Modyfikacja uprawnień	☐ Odebranie uprawnień w systemie informatycznym

Imię i nazwisko użytkownika:	**Wydział/biuro/samodzielne stanowisko**
Opis zakresu uprawnień użytkownika w systemie informatycznym	
Data wystawienia:	Podpis bezpośredniego przełożonego użytkownika systemu:
	Akceptacja ABI

Załącznik nr 3
do Instrukcji Zarządzania Systemem Informatycznym

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRACY W SYSTEMIE INFORMATYCZNYM ORAZ UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Nazwisko , imię	System/aplikacja	Zakres upoważnienia do przetwarzania danych osobowych	Data nadania uprawnień	Data ustania uprawnień	Identyfikator użytkownika

Załącznik nr 4
do Instrukcji Zarządzania
Systemem Informatycznym

WNIOSEK
O UDOSTĘPNIENIE DANYCH ZE ZBIORU DANYCH OSOBOWYCH

1. Wniosek do Starosty Gostyńskiego

2. Wnioskodawca .....
.....
(nazwa firmy i jej siedziba albo nazwisko, imię i adres zamieszkania wnioskodawcy, ew. NIP oraz nr REGON)

3. Podstawa prawna upoważniająca do pozyskania danych albo wskazanie wiarygodnie uzasadnionej potrzeby posiadania danych w przypadku osób innych niż wymienione w art. 29 ust. 1 ustawy o ochronie danych osobowych:.....
.....
..... * □ ew. cd. w załączniku nr.....

4. Wskazanie przeznaczenia dla udostępnionych danych:.....
.....
..... * □ ew. cd. w załączniku nr.....

5. Oznaczenie lub nazwa zbioru, z którego mają być udostępnione dane:.....
.....

6. Zakres żądanych informacji ze zbioru:.....
.....
..... * □ ew. cd. w załączniku nr.....

7. Informacje umożliwiające wyszukanie w zbiorze żądanych danych:.....
.
.....
..... * □ ew. cd. w załączniku nr.....

---

* Jeżeli TAK, to zakreśla kwadrat literą „x”:
(miejsce na znaczki opłaty skarbowej)

.....
(data, podpis i ewentualnie pieczęć wnioskodawcy)

Załącznik nr 5
do Instrukcji Zarządzania
Systemem Informatycznym

Dziennik zawiera opisy wszelkich zdarzeń istotnych dla działania systemu informatycznego w szczególności:

- w przypadku awarii - opis awarii, przyczyna awarii, szkody wynikłe na skutek awarii, sposób usunięcia awarii, opis systemu po awarii, wnioski;
- w przypadku konserwacji systemu – opis podjętych działań, wnioski.

DZIENNIK SYSTEMU INFORMATYCZNEGO
STAROSTWA POWIATOWEGO W GOSTYNIU

Lp	Data i godzina zdarzenia	Opis zdarzenia	Podjęte działania/wnioski	Podpis