Załącznik nr 2
do Zarządzenia nr 7/.....
Starosty Mławskiego
z dnia ...16.03.2010.....

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

I. Procedura nadawania i zmiany uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemach informatycznych oraz wskazanie osoby odpowiedzialnej za te czynności

1.Administrator danych:
nadaje upoważnienie w zakresie dostępu do systemu informatycznego osobie, która w związku z wykonywanymi przez siebie obowiązkami będzie miała dostęp do danych osobowych w systemie, przekazuje wypełniony dokument w postaci papierowej do:

I egz do kadr - celem umieszczenia teczce akt osobowych,
I egz do osoby której upoważnienie dotyczy,
I egz do ABI,

2.Administrator Bezpieczeństwa Informacji (ABI):

aktualizuje ewidencję osób upoważnionych do przetwarzania danych osobowych w systemie informatycznym;

3.Administratorzy Systemu Informatycznego (ASI) tzn. pracownicy zatrudnieni w Starostwie Powiatowym w Mławie na etacie informatyka lub starszego informatyka:

rejestrują użytkownika w systemie i nadają mu określone uprawnienia oraz hasło

4.Użytkownik:
uwierzytelnia się w systemie po podaniu identyfikatora oraz hasła uzyskanego od Informatyka; użytkownik zmienia hasło na swoje, którego nie przekazuje nikomu i może rozpocząć pracę w aplikacji.

5.Użytkownik jest wyrejestrowany z systemu informatycznego w każdym przypadku utraty przez niego uprawnień do dostępu do danych osobowych, co ma miejsce w przypadku:

a) ustania zatrudnienia,
b) zmiany zakresu obowiązków,
c) utraty upoważnienia.

6.Informację pisemną o zatrudnieniu lub ustaniu zatrudnienia, zmianie zakresu obowiązków i utracie upoważnienia, przekazują kadry do ABI z chwilą ich zaistnienia.

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

1. W systemie informatycznym stasuje się uwierzytelniania dwustopniowe; na poziomie:
   b) dostępu do sieci lokalnej,
   c) dostępu do aplikacji.

1. Do uwierzytelnienia użytkownika w systemie na obu poziomach stosuje się hasła.

1. Hasło dostępu da sieci lokalnej składa się, co. najmniej z 4 znaków, zawiera małe i wielkie litery oraz cyfry i znaki specjalne.

2. Hasła nie mogą być powszechnie używanymi sławami. W szczególności nie należy jaka haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.

2. Hasła nie może być ujawniane nawet po utracie przez nie ważności.

3. Zmiana hasła da systemu następuje nie rzadziej, niż co. 30 dni oraz niezwłocznie w przypadku podejrzenia, że hasła mogła zastać ujawniane.

4. Dla każdej osoby upoważnionej instalowany jest odrębny identyfikator i hasła, tak, aby bezpośredni dostęp da danych osobowych przetwarzanych w systemie informatycznym mogła mieć tylko, ta osoba, która pada właściwy identyfikator i hasła.

5. Identyfikator użytkownika jest wpisywany da ewidencji osób upoważnianych da przetwarzania danych osobowych w systemie informatycznym wraz z zakresem upoważnienia oraz datą nadania uprawnień.

3. Aplikacja wymusi na użytkowniku zmianę swojego, hasła, co. 30 dni.

6. System zostanie wyłączany po trzykrotnej próbie nieudanego, logowania się - uzależniane od ustawień BIOS-u.

4. Aplikacja zastanie wyłączana po trzykrotnej próbie nieudanego, logowania się

5. System zastanie wyłączany po określonym czasie logowania.

7. Użytkownik zapisuje swój identyfikator i hasła dostępu da aplikacji zarządzającej systemem administrowania i przekazuje je w kopercie ABI. Koperta zastaje zabezpieczana w sposób uniemożliwiający jej nieuważne otwarcie. ABI przechowuje kopertę w kasecie metalowej w pokoju nr 15B

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

1. Procedura rozpoczęcia pracy

a) uruchomić komputer w systemie podając hasło,
b) uruchomić komputer i załogować się podając swój identyfikator dostępu do sieci,
c) uruchomić aplikację, wpisując swój identyfikator i hasło dostępu uzależnione od programu i rozpocząć pracę.

2. Procedura zawieszenia pracy w systemie

) przy każdorazowym opuszczeniu stanowiska komputerowego,

dopilnować, aby na ekranie nie były wyświetlane dane osobowe,

) przed opuszczaniem miejsca pracy na dłuższy czas użytkownik obowiązany jest poczekać, aż zaktywizuje się wygaszacz ekranu.

3. Procedura zakończenia pracy w systemie

) zarchiwizować dane,

) zamknąć aplikację,

) zamknąć system,

) wyłączyć monitor i drukarkę.

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

4. W cyklu dziennym kopie wykonywane są w serwerze oraz na odrębnym stanowisku komputerowym pełniącym funkcję archiwum.

5. W razie potrzeby kopie zapasowe wykonywane są przez użytkowników aplikacji na zewnętrznych elektronicznych nośnikach informacji.

6. Administratorzy Systemu Informatycznego sprawują nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.

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

8. Dane osobowe w postaci elektronicznej przetwarzane w systemie informatycznym, zapisane na dyskietkach, płytach CD czy dyskach twardych nie mogą być wynoszone poza siedzibę urzędu.

9. Elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych, określony w niniejszym zarządzeniu.

10. Po zakończeniu pracy przez użytkowników systemu elektroniczne nośniki informacji są przechowywane w zamykanych na klucz szafach biurowych lub szafach pancernych.

1. Dane osobowe w postaci elektronicznej, po ustaniu ich użyteczności należy usunąć z nośnika informacji w sposób uniemożliwiający ich ponowne odtworzenie, nie później niż po upływie 3 dni.

2. W przypadku uszkodzenia lub zużycia nośnika elektronicznego zawierającego dane osobowe należy go fizycznie zniszczyć przez spalenie lub rozdrobnienie.

3. Kopie zapasowe zbioru danych osobowych są przechowywane w pokoju nr 15 w szafach pancernych.

7. Dostęp do szaf pancernych mają tylko upoważnieni pracownicy, tj. ABI i ASI.

8. Wydruki, zawierające dane osobowe, należy przechowywać w pokojach stanowiących obszar przetwarzania danych osobowych, określonych w niniejszym zarządzeniu.

9. Wydruki, zawierające dane osobowe, należy zniszczyć przez pocięcie w niszczarce nie później niż po upływie 3 dni, po ich wykorzystaniu chyba, że z odrębnych przepisów wynika obowiązek ich przechowywania.
10. Dane osobowe zapisane w formie papierowej inne niż wydruki z systemu (pisma, ankiety itp.) są przechowywane na podobnych zasadach, co wydruki.

VI. Środki ochrony przed wirusami komputerowymi oraz oprogramowaniem, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

10. Nadzór nad instalowaniem nowego oprogramowania antywirusowego oraz nad bieżącą jego aktualizacją sprawuje Administratorzy Systemu Informatycznego ASI (informatycy).

11. Oprogramowanie zastosowane w systemach informatycznych automatycznie monitoruje występowanie wirusów w trakcie załączania lub wczytywania danych z zewnętrznych nośników informacji

12. Kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.

13. Czynności związane z ochroną antywirusową systemu informatycznego wykonuje Informatyk, wykorzystując w trakcie pracy moduł programu antywirusowego z aktualną bazą antywirusową.

14. Użytkownik systemu importujący dane osobowe do systemu informatycznego z elektronicznego nośnika jest odpowiedzialny za sprawdzenie tych danych pod kątem możliwości występowania wirusów.

15. O każdorazowym wykryciu wirusa przez oprogramowanie antywirusowe użytkownik obowiązany jest niezwłocznie poinformować ABI lub ASI (Informatyka).

16. Po usunięciu wirusa Informatyk sprawdza system informatyczny oraz przywraca go do pełnej funkcjonalności i sprawności.
1. Administratorzy Systemu Informatycznego prowadzą rejestr przypadków zainfekowania komputerów i nośników wykorzystywanych do przetwarzania danych osobowych w systemie.

2. Administratorzy Systemu Informatycznego są odpowiedzialni za aktywowanie i poprawne konfigurowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku: sieci lokalnej, stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci lokalnej.

1. Użytkownikowi systemu zabrania się dokonywania jakichkolwiek zmian konfiguracji w zainstalowanym oprogramowaniu monitorującym wymianę danych na styku tego stanowiska i sieci lokalnej.

2. Ochrona systemu informatycznego używanego w starostwie polega na:
) ochronie przez identyfikator,
) ochronie za pomocą hasła,
) przydzielaniu praw,
) nadawaniu atrybutów.

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

1. W systemie informatycznym odnotowywane są informacje o odbiorcach danych z tego systemu – w odniesieniu do aplikacji gdzie nie jest to możliwe/komórka organizacyjna gdzie przetwarzane są dane osobowe prowadzi rejestr odbiorców danych złego systemu w formie pisemnej .

2. Odbiorcą danych jest każdy, komu udostępnia się dane osobowe, z wyłączeniem:

) osoby, której dane dotyczą
) osoby użytkownika systemu lub innej osoby upoważnionej do przetwarzania danych osobowych w urzędzie
) przedstawiciela, o którym mowa w art. 3 a) ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych podmiotu, któremu powierzono przetwarzanie danych,
) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

3. Odnotowanie obejmuje informacje o:

) nazwie jednostki organizacyjnej lub imieniu i nazwisku osoby, której udostępniono dane,
) zakresie udostępnianych danych,
) dacie udostępnienia.

4. Obowiązek odnotowania ww. informacji spoczywa na użytkowniku systemu, w tym celu wypełnia on odpowiednie pole w bazie danych osobowych lub w rejestrze.

5. Odnotowanie informacji powinno nastąpić niezwłocznie po udostępnieniu danych.

6. Udostępnienie danych osobowych może nastąpić wyłącznie na pisemną prośbę odbiorcy danych.

7. Nadzór nad prawidłowością odnotowywania w systemie ww. informacji sprawuje ABI.

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

1. Odpowiedzialni za przeglądy i konserwacje są ASI i o przeprowadzanych przeglądach i konserwacjach systemu każdorazowo informowany jest ABI, który może nadzorować przebieg prac.

2. Przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego wykonywane są kwartalnie .

3. Nieprawidłowości ujawnione w trakcie tych działań zostaną niezwłocznie usunięte, a ich przyczyny przeanalizowane i przekazane do ABI.

4. Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada Administratorzy Systemu Informatycznego.

5. Sprawdzanie poprawności działania programów i narzędzi programowych przeprowadza się w następujących przypadkach:

) zmiany wersji oprogramowania serwera plików;
) zmiany wersji oprogramowania stanowiska komputerowego użytkownika systemu;
) zmiany systemu operacyjnego serwera plików;
) zmiany systemu operacyjnego stanowisk komputerowego użytkownika systemu;
) wykonania/zmian w projekcie systemu spowodowanych koniecznością naprawy, konserwacji lub modyfikacji systemu

6. Przed dokonaniem zmian w systemie informatycznym należy dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych na testowej bazie danych. Sprawdzenie powinno obejmować:

a) poprawność logowania się do systemu w zależności od posiadanych uprawnień (zasymulować pracę wszystkich typów uprawnień użytkownika)
b) poprawność działania wszystkich elementów aplikacji (menu, zestawienia, formularze, raporty).
c) Poprawność funkcjonowania aplikacji polega na symulacji działania wykonując następujące operacje:
d) wprowadzania danych osobowych
e) edytowania danych osobowych;
f) wyszukiwania. danych osobowych;
g) wydruku danych osobowych.

8. Przegląd przeprowadza/projektant nowego systemu w obecności Administratora Systemu Informatycznego

9. Za prawidłowość przeprowadzenia przeglądów i konserwacji systemu odpowiada Administrator Systemu Informatycznego.
10. Konserwację oprogramowania przeprowadza się po zgłoszeniu przez użytkownika systemu potrzeby wprowadzenia zmian pozwalających utrzymać funkcjonalność systemu w dynamicznie zmieniającym się środowisku pracy.
11. Przed dokonaniem zmian w systemie informatycznym należy dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych na testowej bazie danych na podobnych zasadach jak ma to miejsce w przypadku przeglądu oprogramowania.

IX. Przetwarzanie danych osobowych w zbiorach doraźnych

1. Dostęp do danych osobowych powinien odbywać się poprzez aplikację edytora tekstu lub, gdy zachodzi potrzeba zapisania\danych w innym formacie np. w postaci pliku arkusza kalkulacyjnego, można tego dokonać w doraźnym zbiorze danych osobowych pod warunkiem, że zapisane dane będą
   należycie chronione, tj.
   a) uniemożliwi się dostęp do danych osobom nieuprawnionym,
   b) uniemożliwi się zmiany danych a tym samym zafałszowanie informacji pochodzących z systemu,
   c) zabezpieczy się bezpośredni dostęp do danych hasłem;
2. Doraźny zbiór danych osobowych należy usunąć z nośnika danych, na którym został

utworzony lub zniszczyć nośnik, nie później niż 3 dni po wykorzystaniu danych.
3. Zawiadamiać ABI w przypadku podejrzenia lub stwierdzenia dostępu do zbioru osób nieuprawnionych.
4. Przetwarzać dane w pokojach stanowiących obszar przetwarzania danych osobowych w systemie informatycznym urzędu.

X. Obowiązki administratorów systemu informatycznego

I. Administratorzy Systemu informatycznego są zobowiązani do:
a) wykonywania poleceń Administratora Bezpieczeństwa Informacji w zakresie zarządzania podległymi systemami informatycznymi
b) czuwania nad właściwym eksploatowaniem podległych im systemów informatycznych i bieżącą ich konserwacją oraz przeglądami
c) prowadzenia, uaktualniania na bieżąco oraz przesyłania administratorowi bezpieczeństwa informacji, danych w zakresie

- listy osób biorących udział przy przetwarzaniu danych osobowych
- lokalizacji pomieszczeń w których te dane są przetwarzane, w przypadku zaistnienia jakichkolwiek zmian tych danych
- rodzaju systemów informatycznych funkcjonujących w zakresie ich działania
- listy identyfikatorów osób biorących udział przy przetwarzaniu danych osobowych w podległych im systemach informatycznych
- czynności serwisowych wykonywanych w podległych systemach informatycznych
- zdarzeń wpływających na bezpieczeństwo systemów informatycznych, w tym m.in.

-wykrytych wirusów, koni trojańskich itp.
-oprogramowania nielegalnego lub zainstalowanego bez upoważnienia
-awarii systemu informatycznego lub jego nieprawidłowego działania
-stwierdzenia faktu korzystania z systemu informatycznego przez osobę niepowołaną
-awarii zasilania

d) kontrolowania i zabezpieczenia prawidłowości przebiegu czynności serwisowych w podległych systemach informatycznych, przy czym urządzenia, dyski lub inne nośniki zawierające dane osobowe, pozbawiają przed naprawą zapisu tych danych lub nadzorują ich naprawę
e) pozbawiania zapisu danych osobowych z tych nośników, które przeznaczone są do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania tych danych
f) pozbawiania zapisu danych osobowych lub uszkadzania w sposób uniemożliwiający odczytanie tych nośników, które przeznaczone są do likwidacji
g) instalowania zabezpieczeń w podległych systemach informatycznych wynikających z zaleceń administratora bezpieczeństwa informacji
h) zgłaszania wydziałowym administratorom danych oraz administratorowi bezpieczeństwa informacji potrzeb w zakresie zabezpieczenia podległych im systemów informatycznych
i) postępowania zgodnie z instrukcją w sytuacji naruszenia ochrony danych osobowych
j) kontrolowania procesu okresowego sprawdzania przez administratorów poszczególnych systemów informatycznych kopii awaryjnych pod kątem prawidłowości ich wykonania oraz ich dalszej przydatności do odtworzenia w przypadku awarii
k) znajomości oraz posiadania dokumentacji funkcji poszczególnych systemów informatycznych ze szczególnym uwzględnieniem procedur

- dostępu i modyfikowania do danych osobowych
- zarządzania identyfikatorami i hasłami użytkowników
- wykonywania kopii awaryjnych oraz odtwarzania danych z tych kopii
- generowania wydruków danych osobowych
- dostępu do plików rejestrujących identyfikatory oraz czas logowania użytkowników

II. Administratorzy systemu informatycznego służącego do przetwarzania danych osobowych odpowiadają bieżącą eksploatację tego systemu, a w szczególności za
a) wszystkie czynności związane z ich funkcjonowaniem i modernizacją
b) rejestrowanie i wyrejestrowywanie z systemu użytkowników
oraz projektantów i programistów w czasie instalowania systemu oraz jego modyfikacji
c) przydzielanie uprawnień do poszczególnych funkcji systemu oraz określenie trybu i częstotliwości zmiany haseł
d) procedury wykonywania kopii awaryjnych, określenie ich częstotliwości, zmianę nośników oraz ich właściwe przechowywanie, sprawdzanie poprawności zapisu i likwidację
e) lokalizację sprzętu komputerowego, ustawienie monitorów i drukarek uniemożliwiające wgląd w dane osobom nieupoważnionym lub kradzież wymiennych nośników danych
f) postępowania zgodnie z instrukcją w sytuacji naruszenia ochrony danych osobowych

STAROSTA

Włodzimierz A. Wojnarowski