Zarządzenie Nr 51/2011
Starosty Mławskiego
z dnia 1.12.2011

w sprawie wprowadzenia polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2002r., Nr 101, poz. 926 z późn. zm.) oraz § 3 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) zarządzam, co następuje:

§ 1

Wprowadzam do stosowania w Starostwie Powiatowym w Mławie:

1) Politykę bezpieczeństwa, która stanowi załącznik nr 1 do niniejszego zarządzenia.
2) Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, która stanowi załącznik nr 2 do niniejszego zarządzenia.

§ 2

Wykonanie zarządzenia powierza się Sekretarzowi Powiatu.

§ 3

Traci moc Zarządzenie Nr 7/2010 Starosty Mławskiego z dnia 16 marca 2010r

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

Starosta Mławski
Włodzimierz A. Wojnarowski

Sporządził:
Zbigniew Kowalski
1.12.2011

SEKRETARZ POWIATU
Danuta Antowicz
1.12.2011 r.

RADCA PRAWNY
Bożena Marchel-Połczuska
Nr OLI/524
01.12.2011

Załącznik Nr 1
do Zarządzenia Nr 511/2011
Starosty Mławskiego
z dnia 1.12.2011

POLITYKA BEZPIECZEŃSTWA

1. Definicje

· Zbiór danych osobowych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

· Administrator danych - zadania administratora danych wykonuje Starosta Mławski.

· Administrator Bezpieczeństwa Informacji - osoba wyznaczona przez Administratora danych, odpowiedzialna za bezpieczeństwo danych osobowych.

· Administrator Systemu Informatycznego - osoba odpowiedzialna za bezpieczeństwo danych osobowych w systemie informatycznym w tym: komputery, serwery i oprogramowanie a także sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych w Starostwie Powiatowym w Mławie.

· System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

· Stacja robocza – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie.

· Bezpieczeństwo systemu informatycznego - wdrożenie przez administratora danych lub osobę przez niego uprawnioną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem.

· Przetwarzanie danych osobowych - wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, archiwizowanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.

· Osoba upoważniona - osoba posiadająca upoważnienie wydane przez administratora danych (lub osobę uprawnioną przez niego) i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej w zakresie wskazanym w upoważnieniu (listę osób upoważnionych do przetwarzania danych osobowych posiada administrator bezpieczeństwa informacji).

· Użytkownik systemu - osoba posiadająca uprawnienia do przetwarzania danych osobowych w systemie informatycznym.

· Osoba uprawniona - osoba posiadająca upoważnienie wydane przez administratora danych osobowych do wykonywania w jego imieniu określonych czynności.

· Ustawa – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

· Rozporządzenie - 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.

2.Wykaz budynków, pomieszczeń, części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.

Dane osobowe przetwarzane są w budynku Starostwa Powiatowego w Mławie przy ul. Reymonta 6, przy ul. Wyspiańskiego 9 oraz przy ul. Stary Rynek 10.

lp.	Wydział	Zakres upoważnienia do przetwarzania danych	Forma i miejsce przechowywania danych (budynek, pomieszczenie, komputer, szafka itp..)
1.	Wydział Organizacyjny i Spraw Obywatelskich	*Rejestr zmian imion i nazwisk*	*Zbiór istnieje w formie papierowej* i przechowywany jest w archiwum , Mława, ul. Reymonta 6,
2	Wydział Organizacyjny i Spraw Obywatelskich	*Ewidencja osób podlegających* obowiązkowi służby wojskowej	*Zbiór istnieje w formie papierowej* i przechowywany jest w pok. 26 Mława, ul. Reymonta 6,
3	Wydział Organizacyjny i Spraw Obywatelskich	Oświadczenia o stanie majątkowym osób pełniących funkcje publiczne (zbiór składa się z 2 części)	Zbiór istnieje w formie papierowej w 2 częściach: 1.Zbiór oświadczeń o stanie majątkowym osób pełniących funkcje publiczne bez radnych Powiatu Mławskiego przechowywany jest w szafie pancernej w pok. Nr. 15 B, a w formie informatycznej na komputerze (zał. Nr 3) w pok. 15 B Mława, ul. Reymonta 6 oraz 2. Zbiór oświadczeń o stanie majątkowym osób pełniących funkcje publiczne w zakresie Radnych Powiatu Mławskiego przechowywane są w formie papierowej w szafie w pok. nr. 24 (Biuro Rady)
4	Wydział Organizacyjny i Spraw Obywatelskich	Skład osobowy Rejonowego Komitetu Przeciwpowodziowego w Mławie	Zbiór w formie papierowej przechowywany jest w szafie w pok. Nr. 26, Mława, ul. Reymonta 6

lp.	Wydział	*Zakres upoważnienia do* przetwarzania danych	Forma i miejsce przechowywania danych (budynek, pomieszczenie, komputer, szafka itp..)
5	Wydział Organizacyjny i Spraw Obywatelskich	Zbiór akt osobowych pracowników Starostwa Powiatowego w Mławie oraz kierowników jednostek organizacyjnych Powiatu Mławskiego z wyłączeniem dyrektorów szkół ponadgimazjalnych. *Nie podlega zgłaszaniu do GIODO* – Art. 43, ust 1, pkt 4 ustawy o ochr. danych osob. (Dz.U.2002. Nr 101, poz. 926)	Pliki w formie papierowej przechowywane są w szafie pancernej w pok. Nr. 15 B, Mława, ul. Reymonta 6
6	Wydział Organizacyjny i Spraw Obywatelskich	Lista osób ubiegających się o wydanie paszportu Nie podlega zgłaszaniu do GIODO – Art. 43, ust 1, pkt 2b ustawy o ochr. danych osob. (Dz.U.2002. Nr 101, poz. 926)	Zbiór istnieje w formie papierowej i przechowywany jest w archiwum , Mława, ul. Reymonta 6,
7	Wydział Rolnictwa i Środowiska	Zbiór danych dotyczących właścicieli reproduktorów	Zbiór danych w formie papierowej przechowywany w pomieszczeniu biurowym Wydz.Rol. I Środ., pok. 1 A, biurko osoby upoważnionej, Mława, ul. Reymonta 6
8	Wydział Rolnictwa i Środowiska	Zbiór danych dotyczących właścicieli lasów nie stanowiących własności Skarbu Państwa	Zbiór danych w formie papierowej przechowywany w pomieszczeniu biurowym Wydz.Rol. i Środ., pok. 1 B, w szafie, Mława, ul. Reymonta 6
9	Wydział Rolnictwa i Środowiska	Ewidencja osób korzystających z wód powierzchniowych i podziemnych oraz urządzeń wodnych	Zbiór danych w formie papierowej przechowywany w pomieszczeniu biurowym Wydz.Rol. i Środ., pok. 1 A, w szafie, Mława, ul. Reymonta 6
10	Wydział Rolnictwa i Środowiska	Rejestr zwierząt i roślin podlegających ograniczeniom na podstawie umów międzynarodowych	Zbiór danych w formie papierowej przechowywany w pomieszczeniu biurowym Wydz.Rol. i Środ., pok. 1 A, biurko osoby upoważnionej, Mława, ul. Reymonta 6
11	Wydział Rolnictwa i Środowiska	Ewidencja osób związanych z ochroną, chowem, hodowlą i połowem ryb w wodach śródlądowych	Zbiór danych w formie papierowej przechowywany w pomieszczeniu biurowym Wydz.Rol. i Środ., pok. 1 A, szafa osoby upoważnionej, Mława, ul. Reymonta 6
12	Wydział Rolnictwa i Środowiska	Rejestr posiadaczy chartów rasowych i ich mieszańców	Zbiór danych w formie papierowej przechowywany w pomieszczeniu biurowym Wydz.Rol. i Środ., pok. 1 A, szafa osoby upoważnionej, Mława, ul. Reymonta 6

lp.	Wydział	Zakres upoważnienia do przetwarzania danych	Forma i miejsce przechowywania danych (budynek, pomieszczenie, komputer, szafka itp..)
13	Wydział Geodezji, Katastru i Gospodarki Nieruchomościami	Ewidencja gruntów i budynków	Num. baza danych na serwerze w pomieszczeniu serwera, komputery (zał. 3) podłączone do serwera , papierowe dowody zmian zawierające dane osobowe, pokoje nr 10, 11, 13, 14, Mława, ul.Stary Rynek 10
14	Wydział Geodezji, Katastru i Gospodarki Nieruchomościami	Ewidencja zgłoszeń robót geodezyjnych i uzgodnień dokumentacji projektowej	Num. baza danych na serwerze w pomieszczeniu serwera, komputery (zał. 3) podłączone do serwera, papierowe dowody zmian zawierające dane osobowe, pok. nr 1, 2, 3, Mława, ul.Stary Rynek 10
15	Wydział Geodezji, Katastru i Gospodarki Nieruchomościami	Decyzje z zakresu gospodarki nieruchomościami	Zbiory w formie papierowej w pokojach 4, 11, 14, Mława, ul.Stary Rynek 10
16	Wydział Geodezji, Katastru i Gospodarki Nieruchomościami	Decyzje o nieodpłatnym przeniesieniu własności nieruchomości	Zbiory w formie papierowej w pokojach 4, 11, 14, Mława, ul.Stary Rynek 10
17	Wydział Geodezji, Katastru i Gospodarki Nieruchomościami	Decyzje o zezwoleniu na wyłączenie gruntów z produkcji rolnej	Zbiory w formie papierowej w pokojach 4, 11, 14, Mława, ul.Stary Rynek 10
18	Wydział Edukacji i Zdrowia	Ewidencja Pracowników Placówek Oświatowych (zbiór składa się z 4 części)	Zbiór istnieje w 4 częściach w systemie informatycznym na komputerach (zał. 3) oraz formie papierowej: kartoteki, skorowidze, księgi przechowywane w szafach w pomieszczeniu nr 7, pokój B (drugi po prawej od wejścia), Mława, ul. Reymonta 6 1.Ewidencja Pracowników Placówek Oświatowych w zakresie I LO i O.Sz.W. 2.Ewidencja Pracowników Placówek Oświatowych w zakresie PPP, ZS nr 4, PODN 3.Ewidencja Pracowników Placówek Oświatowych w zakresie ZS nr 2, Bursa Szkolna 4. Ewidencja Pracowników Placówek Oświatowych w zakresie ZS nr 1, ZS nr 3

lp.	Wydział	*Zakres upoważnienia do* przetwarzania danych	Forma i miejsce przechowywania danych (budynek, pomieszczenie, komputer, szafka itp..)
19	Wydział Edukacji i Zdrowia	Baza Danych Oświatowych	Zbiór istnieje w systemie informatycznym na komputerze (zał. 3) (komputer obsługujący SIO) oraz formie papierowej:kartoteki, skorowidze, księgi przechowywane w szafie, w pomieszczeniu nr 7, pokój główny, Mława, ul. Reymonta 6
20	Wydział Edukacji i Zdrowia	Ewidencja podmiotów korzystających ze środków PFRON	Zbiór istnieje w formie papierowej, przechowywany w szafie w pomieszczeniu nr 7, pokój C (pierwszy po lewej od wejścia), Mława, ul. Reymonta 6
21	Wydział Edukacji i Zdrowia	Wyrównywanie szans edukacyjnych poprzez programy stypendialne	Zbiór istnieje w systemie informatycznym na komputerze (zał. 3) oraz formie papierowej: kartoteki, skorowidze, księgi przechowywane w szafach w pomieszczeniu nr 7, pokój C (pierwszy po lewej od wejścia), Mława, ul. Reymonta 6
22	Wydział Finansowy	Płace Nie podlega zgłaszaniu do GIODO – Art. 43, ust 1, pkt 4 ustawy o ochr. danych osob. (Dz.U.2002. Nr 101, poz. 926)	Zbiór istnieje w systemie informatycznym na komputerze (zał. 3) oraz formie papierowej: segregatory, teczki przechowywane w szafach w pomieszczeniu nr 6, (pierwsza po lewej od wejścia oraz w biurku), Mława, ul. Reymonta 6
23	Wydział Finansowy	Płatnik-Starostwo Powiatowe w Mławie Nie podlega zgłaszaniu do GIODO – Art. 43, ust 1, pkt 4 ustawy o ochr. danych osob. (Dz.U.2002. Nr 101, poz. 926)	Zbiór istnieje w systemie informatycznym komputerze (zał. 3) oraz formie papierowej: segregatory, teczki przechowywane w szafach w pomieszczeniu nr 6, (pierwsza po lewej od wejścia oraz w biurku), Mława, ul. Reymonta 6
24	Wydział Infrastruktury	Ewidencja rozpoczynanych i oddanych obiektów do *użytkowania z zakresu prawa* budowlanego (archiwizacja do dnia 10.07.2003r.)	Zbiór istnieje w formie papierowej i przechowywany jest w archiwum, Mława, ul.Reymonta 6
25	Wydział Infrastruktury	Rejestr decyzji pozwoleń na budowę z zakresu prawa budowlanego	Zbiór istnieje w formie papierowej (zeszyty) w pokoju nr 25A, w szafie, Mława, ul. Reymonta 6
26	Wydział Infrastruktury	Rejestr wniosków pozwoleń z zakresu prawa budowlanego	Zbiór istnieje w formie papierowej (zeszyty) w pokoju nr 25A, w szafie

lp.	Wydział	Zakres upoważnienia do przetwarzania danych	Forma i miejsce przechowywania danych (budynek, pomieszczenie, komputer, szafka itp..)
27	Wydział Komunikacji	Ewidencja kierowców	Zbiór istnieje w formie informatycznej na komputerach (zał. 3) w pomieszczeniach 1,2(serwer),8 a także w formie papierowej w pok. 1,2,8 oraz w archiwum na ul.Reymonta 6 w trzech pomieszczeniach, Mława, ul. Wyspiańskiego 9
28	Wydział Komunikacji	Ewidencja pojazdów	Zbiór istnieje w formie informatycznej na komputerach (zał. 3) w pomieszczeniach 2(serwer),3,5,6,7 a także w formie papierowej w pok. 3,5,6,7 oraz w archiwum na ul.Reymonta 6 w pomieszczeniach, Mława, ul. Wyspiańskiego 9
29	Wydział Komunikacji	Ewidencja kart parkingowych	Zbiór istnieje w formie papierowej, pokój nr 8, Mława, ul. Wyspiańskiego 9
30	Wydział Komunikacji	Ewidencja instruktorów jazdy	Zbiór istnieje w formie papierowej, pokój nr 8, Mława, ul. Wyspiańskiego 9
31	Wydział Komunikacji	Ewidencja zaświadczeń na krajowy przewóz rzeczy na potrzeby własne	Zbiór istnieje w formie papierowej, pokój nr 4, Mława, ul. Wyspiańskiego 9
32	Wydział Komunikacji	Ewidencja licencji na krajowy przewóz rzeczy	Zbiór istnieje w formie papierowej, pokój nr 4, Mława, ul. Wyspiańskiego 9
33	Wydział Komunikacji	Ewidencja licencji na krajowy drogowy przewóz osób	Zbiór istnieje w formie papierowej, pokój nr 4,Mława, ul. Wyspiańskiego 9

3.Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

Dane osobowe przetwarzane są w budynkach Starostwa Powiatowego w Mławie przy ul. Reymonta 6, Wyspiańskiego 9 i Stary Rynek 10.

lp.	Zakres upoważnienia do przetwarzania danych	Nazwa programu zastosowanego do przetwarzania zbioru danych osob.	Autor programu
1.	Rejestr zmian imion i nazwisk	Nie dotyczy	Nie dotyczy
2	Ewidencja osób podlegających obowiązkowi służby wojskowej	Nie dotyczy	Nie dotyczy

lp.	Zakres upoważnienia do przetwarzania danych	Nazwa programu *zastosowanego do* przetwarzania zbioru danych osob.	Autor programu
3	Oświadczenia o stanie majątkowym osób pełniących funkcje publiczne (zbiór składa się z 2 części)	Nie dotyczy	Nie dotyczy
4	Skład osobowy Rejonowego Komitetu Przeciwpowodziowego w Mławie	Nie dotyczy	Nie dotyczy
5	Zbiór akt osobowych pracowników Starostwa Powiatowego w Mławie oraz kierowników jednostek organizacyjnych Powiatu Mławskiego z wyłączeniem dyrektorów szkół ponadgimazjalnych. Nie podlega zgłaszaniu do GIODO – Art. 43, ust 1, pkt 4 ustawy o ochr. danych osob. (Dz.U.2002. Nr 101, poz. 926)	Nie dotyczy	Nie dotyczy
6	Lista osób ubiegających się o wydanie paszportu Nie podlega zgłaszaniu do GIODO – Art. 43, ust 1, pkt 2b ustawy o ochr. danych osob. (Dz.U.2002. Nr 101, poz. 926)	Nie dotyczy	Nie dotyczy
7	Zbiór danych dotyczących właścicieli reproduktorów	Nie dotyczy	Nie dotyczy
8	Zbiór danych dotyczących właścicieli lasów nie stanowiących własności Skarbu Państwa	Nie dotyczy	Nie dotyczy
9	Ewidencja osób korzystających z wód powierzchniowych i podziemnych oraz urządzeń wodnych	Nie dotyczy	Nie dotyczy
10	Rejestr zwierząt i roślin podlegających ograniczeniom na podstawie umów międzynarodowych	Nie dotyczy	Nie dotyczy
11	Ewidencja osób związanych z ochroną, chowem, hodowlą i połowem ryb w wodach śródlądowych	Nie dotyczy	Nie dotyczy
12	Rejestr posiadaczy chartów rasowych i ich mieszańców	Nie dotyczy	Nie dotyczy

lp.	Zakres upoważnienia do przetwarzania danych	Nazwa programu zastosowanego do przetwarzania zbioru danych osob.	Autor programu
13	Ewidencja gruntów i budynków	EWOPIS, EWMAPA	GEOBIOD Katowice
14	Ewidencja zgłoszeń robót geodezyjnych i uzgodnień dokumentacji projektowej	System OŚRODEK	GEOBIOD Katowice
15	Decyzje z zakresu gospodarki nieruchomościami	Nie dotyczy	Nie dotyczy
16	Decyzje o nieodpłatnym przeniesieniu własności nieruchomości	Nie dotyczy	Nie dotyczy
17	Decyzje o zezwoleniu na wyłączenie gruntów z produkcji rolnej	Nie dotyczy	Nie dotyczy
18	Ewidencja Pracowników Placówek Oświatowych (zbiór składa się z 4 części)	PŁATNIK, KADRY I PŁACE, FK	PROKOM, WOI Warszawa, PIK
19	Baza Danych Oświatowych	SIO	MENiS
20	Ewidencja podmiotów korzystających ze środków PFRON	Nie dotyczy	Nie dotyczy
21	Wyrównywanie szans edukacyjnych poprzez programy stypendialne	PEFS	Urząd Marszałkowski
22	Płace Nie podlega zgłaszaniu do GIODO – Art. 43, ust 1, pkt 4 ustawy o ochr. danych osob. (Dz.U.2002. Nr 101, poz. 926)	KADRY I PŁACE	Wojewódzki Ośrodek Informatyki w Warszawie, Wydział Zamiejscowy w Ciechanowie
23	Płatnik-Starostwo Powiatowe w Mławie Nie podlega zgłaszaniu do GIODO – Art. 43, ust 1, pkt 4 ustawy o ochr. danych osob. (Dz.U.2002. Nr 101, poz. 926)	PŁATNIK	PROKOM Software S.A.
24	Ewidencja rozpoczynanych i oddanych obiektów do użytkowania z zakresu prawa budowlanego (archiwizacja do dnia 10.07.2003r.)	Nie dotyczy	Nie dotyczy

lp.	Zakres upoważnienia do przetwarzania danych	Nazwa programu *zastosowanego do* przetwarzania zbioru danych osob.	Autor programu
25	Rejestr decyzji pozwoleń na budowę z zakresu prawa budowlanego	Nie dotyczy	Nie dotyczy
26	Rejestr wniosków pozwoleń z zakresu prawa budowlanego	Nie dotyczy	Nie dotyczy
27	Ewidencja kierowców	CEPIK, Moduł Ewidencji Osób Uprawnionych, Podsystem Obsługi Zamówień	Hawlett Packard
28	Ewidencja pojazdów	CEPIK, Moduł Ewidencji Osób Uprawnionych, Podsystem Obsługi Zamówień	Hawlett Packard
29	Ewidencja kart parkingowych	Nie dotyczy	Nie dotyczy
30	Ewidencja instruktorów jazdy	Nie dotyczy	Nie dotyczy
31	Ewidencja zaświadczeń na krajowy przewóz rzeczy na potrzeby własne	Nie dotyczy	Nie dotyczy
32	Ewidencja licencji na krajowy przewóz rzeczy	Nie dotyczy	Nie dotyczy
33	Ewidencja licencji na krajowy drogowy przewóz osób	Nie dotyczy	Nie dotyczy

4.Opis struktury zbiorów danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania pomiędzy nimi.

L.p.	Nazwa zbioru danych osobowych	Zawartość pól danych osobowych
1.	Rejestr zmian imion i nazwisk	1.Nazwiska i imiona 2.Data i miejsce urodzenia 3.Nowe personalia 4.Adres zamieszkania
2.	Ewidencja osób podlegających obowiązkowi służby wojskowej	1.numer pozycji z księgi orzeczeń lekarskich 2.nazwisko i imię oraz imię ojca poborowego 3.rok urodzenia poborowego 4.miejsce stałego lub czasowego pobytu (dokładny adres) poborowego 5.datę stawienia się do poboru 6.kategorię zdrowia 7.numer książeczki wojskowej
3.	Oświadczenia o stanie majątkowym osób pełniących funkcje publiczne (zbiór składa się z 2 części)	1.nazwiska i imiona, 2.nazwisko rodowe i z poprzedniego małżeństwa, 3.imiona rodziców, 4.data urodzenia, miejsce urodzenia 5..miejsce zatrudnienia, stanowisko, funkcja 6.zasoby pieniężne 7..dom, mieszkanie, gospodarstwo rolne bądź inne nieruchomości wraz z tytułem prawnym 8.posiadane udziały w spółkach handlowych oraz dochody z tego tytułu 9.akcje w spółkach handlowych i dochody z tego tytułu 10.mienie nabyte od Skarbu Państwa czy innych państwowych osób prawnych , jednostek samorządu terytorialnego 11.prowadzenie działalności gospodarczej i dochody z tego tytułu 12.zarządzanie działalnością gospodarczą i dochody z tego tytułu 13.bycie członkiem rad nadzorczych, zarządów, komisji rewizyjnych w spółkach handlowych, w spółdzielniach, fundacjach i uzyskane z tego tytułu dochody 14.inne dochody osiągane z tytułu wynagrodzenia 15.składniki mienia ruchomego o wartości powyżej 10 tys. zł 16.zobowiązania pieniężne o wartości powyżej 10 tys. zł, w tym kredyty i pożyczki 17.adres zamieszkania osoby składającej oświadczenie 18.miejsce położenia nieruchomości

L.p.	Nazwa zbioru danych osobowych	Zawartość pól danych osobowych
4	Skład osobowy Rejonowego Komitetu Przeciwpowodziowego w Mławie	1.Nazwiska i imiona 2.adres zamieszkania lub pobytu
5	Zbiór akt osobowych pracowników Starostwa Powiatowego w Mławie oraz kierowników jednostek organizacyjnych Powiatu Mławskiego z wyłączeniem dyrektorów szkół ponadgimazjalnych. Nie podlega zgłaszaniu do GIODO – Art. 43, ust 1, pkt 4 ustawy o ochr. danych osob. (Dz.U.2002. Nr 101, poz. 926)	1.Nazwisko i imię 2.imiona rodziców 3.data urodzenia 4.miejsce urodzenia 5.adres zamieszkania i pobytu 6.zawód 7.wykształcenie 8.numer telefonu
6	Lista osób ubiegających się o wydanie paszportu Nie podlega zgłaszaniu do GIODO – Art. 43, ust 1, pkt 2b ustawy o ochr. danych osob. (Dz.U.2002. Nr 101, poz. 926)	1.Nazwisko i imię 2.PESEL
7	Zbiór danych dotyczących właścicieli reproduktorów	1.Nazwisko i Imię 2.Adres zamieszkania
8	Zbiór danych dotyczących właścicieli lasów nie stanowiących własności Skarbu Państwa	1.Nazwisko i Imię 2.Imiona rodziców 3.Data urodzenia 4.Adres zamieszkania 5.Numer ewidencyjny 6.PESEL 7.Seria i nr dowodu osobistego
9	Ewidencja osób korzystających z wód powierzchniowych i podziemnych oraz urządzeń wodnych	1.Nazwisko i Imię 2.Adres zamieszkania
10	Rejestr zwierząt i roślin podlegających ograniczeniom na podstawie umów międzynarodowych	1.Nazwisko i Imię 2.Adres zamieszkania
11	Ewidencja osób związanych z ochroną, chowem, hodowlą i połowem ryb w wodach śródlądowych	1.Nazwisko i Imię 2.Data urodzenia 3.Adres zamieszkania
12	Rejestr posiadaczy chartów rasowych i ich mieszańców	1.Nazwisko i Imię 2.Adres zamieszkania
13	Ewidencja gruntów i budynków	1.Imię i nazwisko, 2.imiona rodziców, 3.Adres zamieszkania 4.Nr PESEL,

L.p.	Nazwa zbioru danych osobowych	Zawartość pól danych osobowych
		5.Nr NIP 6.Nr dowodu osobistego
14	Ewidencja zgłoszeń robót geodezyjnych i uzgodnień dokumentacji projektowej	1Imię i nazwisko, 2.imiona rodziców, 3.Adres zamieszkania 4.Nr NIP
15	Decyzje z zakresu gospodarki nieruchomościami	1.Imię i nazwisko, 2.Adres zamieszkania
16	Decyzje o nieodpłatnym przeniesieniu własności nieruchomości	1.Imię i nazwisko, 2.Adres zamieszkania
17	Decyzje o zezwoleniu na wyłączenie gruntów z produkcji rolnej	1.Imię i nazwisko, 2.Adres zamieszkania
18	Ewidencja Pracowników Placówek Oświatowych (zbiór składa się z 4 części)	1.nazwiska i imiona, 2.imiona rodziców, 3.data urodzenia, 4.miejsce urodzenia, 5.adres zamieszkania lub pobytu, 6.PESEL, 7.NIP, 8.miejsce pracy, 9.zawód, 10.wykształcenie, 11.seria i numer dowodu osobistego, 12.numer telefonu;: 13.przynależność związkowa;
19	Baza Danych Oświatowych	1.Data urodzenia, 2.PESEL, 3.miejsce pracy, 4.zawód, 5.wykształcenie;
20	Ewidencja podmiotów korzystających ze środków PFRON	1.nazwiska i imiona, 2.data urodzenia, 3.adres zamieszkania lub pobytu, 4.numer ewidencyjny PESEL, 5.miejsce pracy, 6.zawód, wykształcenie, 7.seria i numer dowodu osobistego; 8.numer rachunku bankowego, 9.numer telefonu, 10.wysokość dochodów
21	Wyrównywanie szans edukacyjnych poprzez programy stypendialne	1.nazwiska i imiona, 2.imiona rodziców, 3.data urodzenia, 4.miejsce urodzenia, 5.adres zamieszkania lub pobytu,

L.p.	Nazwa zbioru danych osobowych	Zawartość pól danych osobowych
		6.PESEL, 7.NIP, 8.wykształcenia, 9.seria i numer dowodu osobistego, 10.numer telefonu, 11.miejsce nauki, 12.dochody członków rodziny, 13.stan cywilny
22	Płace Nie podlega zgłaszaniu do GIODO – Art. 43, ust 1, pkt 4 ustawy o ochr. danych osob. (Dz.U.2002. Nr 101, poz. 926)	1.Imię i nazwisko 2.Imiona, nazw. rodziców 3.NIP 4.PESEL 5.Adres 6.Forma zatrudnienia 7.Wynagrodzenie, składki i inne elementy związane z wynagrodzeniem
23	Płatnik – Starostwo Powiatowe w Mławie Nie podlega zgłaszaniu do GIODO – Art. 43, ust 1, pkt 4 ustawy o ochr. danych osob. (Dz.U.2002. Nr 101, poz. 926)	1.Imię i nazwisko 2.Imiona, nazw. rodziców 3.NIP 4.PESEL 5.Adres 6.Forma zatrudnienia 7.Wynagrodzenie, składki i inne elementy związane z wynagrodzeniem
24	Ewidencja rozpoczynanych i oddanych obiektów do użytkowania z zakresu prawa budowlanego (archiwizacja do dnia 10.07.2003r.)	1.Nazwisko i imię 2.Adres zamieszkania lub pobytu 3.Adres budowy
25	Rejestr decyzji pozwoleń na budowę z zakresu Prawa Budowlanego	1.Nazwisko i imię 2.Adres zamieszkania lub pobytu
26	Rejestr wniosków pozwoleń z zakresu Prawa Budowlanego	1.Nazwisko i imię 2.Adres zamieszkania lub pobytu
27	Ewidencja kierowców	1.Imię, nazwisko, 2.adres, 3.data urodzenia, 4.numer PESEL
28	Ewidencja pojazdów	1.Imię, nazwisko, 2.adres, 3.data urodzenia, 4.numer PESEL
29	Ewidencja kart parkingowych	1.Imię, nazwisko, 2.adres
30	Ewidencja instruktorów jazdy	1.Imię, nazwisko, 2.adres, 3.numer PESEL
31	Ewidencja zaświadczeń na krajowy przewóz rzeczy na potrzeby własne	1.Nazwisko i imię 2.adres

L.p.	Nazwa zbioru danych osobowych	Zawartość pól danych osobowych
32	Ewidencja licencji na krajowy przewóz rzeczy	1.Nazwisko i imię 2.adres
33	Ewidencja licencji na krajowy drogowy przewóz osób	1.Nazwisko i imię 2.adres

5.Sposób przepływu danych pomiędzy poszczególnymi systemami

Brak przepływu danych pomiędzy poszczególnymi systemami

6.Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

A. Środki ochrony fizycznej

1. Budynki urzędu, w których zlokalizowany jest obszar przetwarzania danych osobowych otwierane są przed rozpoczęciem pracy urzędu oraz zamykane po zakończeniu pracy przez upoważnionych pracowników. Osoby te odpowiedzialne są za klucze. Przy otwieraniu i zamykaniu wyłączany i włączany jest alarm elektroniczny.
2. Budynki opisane w pkt.1 zlokalizowane są w trzech miejscach pod następującymi adresami:
   1)Mława, ul.Reymonta 6
   2)Mława, ul.Wyspiańskiego 9
   3)Mława, ul.Stary Rynek 10
3. Urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych zamkami.
4. Przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osoby zatrudnionej przy przetwarzaniu lub w obecności zwierzchnika służbowego takiej osoby.
5. Po godzinach pracy dopuszcza się pracę w pomieszczeniach, w których przetwarzane i przechowywane są zbiory danych osobowych jedynie osobom zatrudnionych przy sprzątaniu i konserwacji, upoważnionych do przebywania w tych pomieszczeniach. Przed i po wypełnieniu w/w czynności pomieszczenia powinny być zamknięte.
6. Pomieszczenia w których zbiory danych osobowych nie są zabezpieczone w zamykanych szafach mogą być sprzątane tylko w obecności upoważnionego pracownika w godzinach obowiązującego czasu pracy. Po zakończeniu pracy i zamknięciu pomieszczenia, klucz od tego pokoju zabierany jest przez pracownika zatrudnionego przy przetwarzaniu danych osobowych.
7. W czasie sprzątania pomieszczeń po obowiązujących godzinach pracy wejście do budynku musi być zamknięte. Zabronione jest wpuszczanie i przebywanie w budynku jakiejkolwiek nieupoważnionej osoby.
8. Po zakończeniu pracy zbiory danych osobowych będące w formie papierowej powinny być zamknięte na klucz (szafy, biurka) a następnie całe pomieszczenie powinno być w ten sam sposób zamknięte, a klucz od pomieszczenia oddany osobie wymienionej w pkt. 5.
9. Po skończeniu pracy klucze od szaf i biurek w których znajdują się zbiory danych osobowych, po ich zamknieciu powinny być zbierane w jedno miejsce np. jedna z szaf. Klucz od tej szafy powinien być zabrany przez pracownika zajmującego się przetwarzaniem tych zbiorów. W przypadku braku takich zabezpieczeń pracownik

wychodzący ostatni zamyka całe pomieszczenie na klucz i zabiera go ze sobą (nie oddaje go osobie wymienionej w pkt. 1).

10. Przy rozpoczynaniu pracy klucze od pomieszczeń pobierane są od osoby odpowiedzialnej za otwarcie budynków wymienionej w punkcie 1.
11. Pomieszczenia, o których mowa w punkcie 4, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.
12. W przypadku przebywania osób postronnych w pomieszczeniach, o których mowa wyżej, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.
13. Do przebywania w pomieszczeniu serwera uprawnieni są: Administratorzy Systemu Informatycznego, Administrator Bezpieczeństwa Informacji oraz Administrator Danych.
14. Przebywanie w pomieszczeniu serwera osób nieuprawnionych (konserwator, elektryk, sprzątaczka i inni) dopuszczalne jest tylko w obecności Administratora Systemu Informatycznego, a w przypadku ich nieobecności – w obecności osoby pisemnie upoważnionej przez kierownika urzędu.

B. Środki sprzętowe, informatyczne i telekomunikacyjne.

1. Każdy dokument papierowy na którym znajdują się dane osobowe przeznaczony do wyrzucenia powinien być uprzednio zniszczony w sposób uniemożliwiający jego odczytanie (np. przy pomocy niszczarki dokumentów).
2. Urządzenia wchodzące w skład systemu informatycznego podłączone są do odrębnego obwodu elektrycznego, zabezpieczonego na wypadek zaniku napięcia albo awarii w sieci zasilającej centralnym UPS-em.
3. Zastosowano odrębny komputer w celu archiwizacji danych z poszczególnych komputerów użytkowników.
4. Na wszystkich serwerach oraz stacjach roboczych zainstalowano oprogramowanie antywirusowe. Poczta elektroniczna wpływająca do Urzędu skanowana jest programem antywirusowym przed przesłaniem jej do Użytkownika.
5. Archiwizacja wykonywana jest na odrębnym komputerze zabezpieczone hasłem w zamykanym pomieszczeniu.
6. Komputery zabezpieczone są hasłami, które znane sa tylko użytkownikowi danego komputera. Co 30 dni użytkownik zmienia hasła i przekazuje je w zamkniętej kopercie Administratorom Systemu Informacji.

C. Środki ochrony w ramach oprogramowania systemu.

1. Dostęp fizyczny do baz danych osobowych zastrzeżony jest wyłącznie dla osób zajmujących się obsługą informatyczną Urzędu.
2. Konfiguracja systemu umożliwia Użytkownikom końcowym dostęp do danych osobowych jedynie za pośrednictwem aplikacji.
3. System informatyczny pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu.
4. W sieciowym systemie operacyjnym zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do sieci.

D. Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych.

1. Zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji, chyba, że program tego nie przewiduje – wówczas jedynym środkiem zabezpieczenia jest hasło systemowe.
2. Dla każdego Użytkownika systemu jest ustalony odrębny identyfikator.
3. Zdefiniowano Użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (unikalny identyfikator i hasło).

E. Środki ochrony w ramach systemu Użytkowego.

1. Zastosowano wygaszanie ekranu w przypadku dłuższej nieaktywności Użytkownika.
2. Komputer, z którego możliwy jest dostęp do danych osobowych zabezpieczony jest hasłem uruchomieniowym.

F. Środki organizacyjne.

1. Wyznaczono Administratora Bezpieczeństwa Informacji (ABI), osoba odpowiedzialna za bezpieczeństwo przetwarzanych danych osobowych w Starostwie Powiatowym w Mławie z wyłączeniem systemu i procedur informatycznych.
2. Wyznaczono Administratorów Systemu Informatycznego (ASI), którzy odpowiedzialni są za bezpieczeństwo przetwarzanych danych osobowych w systemie i procedurach informatycznych. Ponadto odpowiadają za zabezpieczenie komputerów, serwerów i oprogramowania a także sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych. Administrator Systemu Informatycznego przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnego upoważnienia kierownika urzędu określającego zakres uprawnień pracownika.
3. Osoby przyjmowane do pracy lub wobec których zmieniono zakres czynności w ten sposób że powinny być upoważnione do przetwarzania danych osobowych są zgłoszone przez pracownika odpowiedzialnego za sprawy osobowe do przeszkolenia przez ABI zanim dopuszczone będą do pracy z tymi zbiorami danych. Szkolenie to obejmuje zakres obowiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych w systemie informatycznym.
4. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych.
5. Wprowadzono instrukcję zarządzania systemem informatycznym.
6. Wprowadzono instrukcję postępowania w sytuacji naruszenia systemu ochrony danych osobowych
7. Wprowadzono obowiązek rejestracji wszystkich przypadków awarii systemu, działań konserwacyjnych w systemie oraz naprawy systemu.
8. Określono sposób postępowania z nośnikami informacji.

7. Instrukcja w sprawie zarządzania oprogramowaniem

1. Oprogramowanie używane w systemie informatycznym musi posiadać aktualną licencję
2. Oprogramowanie nie posiadające licencji powinno być zgłoszone przez użytkownika i natychmiast usunięte przez Administratorów Systemu Informatycznego

3. Komputery powinny być zabezpieczone przed możliwością wgrywania nie licencjonowanego oprogramowania na ile pozwala na to środowisko informatyczne komputera, w którym pracuje użytkownik.
4. Odpowiedzialność za posiadanie zainstalowanych nie licencjonowanych programów ponosi użytkownik.
5. Administratorzy Systemu Informatycznego sporządzają i aktualizują listę oprogramowania wraz z lokalizacją użytkowania tego oprogramowania
6. Administratorzy Systemu Informatycznego przechowują elektroniczne nośniki oprogramowania, które używane jest w systemie informatycznym. W przypadku licencji na użytkownika na nośniku wpisywane jest imię i nazwisko danego użytkownika.
7. Każdy elektroniczny nośnik oprogramowania ma wpisaną na nośniku pozycję ewidencyjną odpowiadającą numeracji na liście wyszczególnionej w pkt. 5 oraz numer komputera, na którym użytkowane jest to oprogramowanie.
8. Elektroniczne nośniki, na których zapisane jest oprogramowanie powinno być przechowywane w zamykanych szafkach w pomieszczeniu serwerowni.
9. Kopie oprogramowania o ile pozwalają na to przepisy licencyjne mogą być wykonane tylko przez Administratorów Systemu Informatycznego i oznaczone zgodnie z punktem 6.
10. Administratorzy Systemu Informatycznego co najmniej raz na pół roku przeprowadzają kontrolę oprogramowania u użytkowników i co najmniej raz na 3-miesiące aktualizują listę oprogramowania wymienioną w pkt. 5
11. Za wdrożenie i aktualizację niniejszej instrukcji odpowiadają Administratorzy Systemu Informatycznego

8. Instrukcja postępowania w sytuacji naruszenia systemu ochrony danych osobowych

a) Użytkownik modułów komputerowych zobowiązany jest zawiadomić Administratora Systemu Informatycznego, o każdym naruszeniu zabezpieczenia systemu polegającym na:
- naruszeniu hasła dostępu (system nie reaguje na hasło lub je ignoruje - usunięty mechanizm hasła),
- częściowym lub całkowitym braku bazy danych
- brak możliwości uruchomienia właściwej aplikacji (programu komputerowego),
- zmianie położenia komputerów
- kradzieży z pomieszczenia, w którym znajduje się sprzęt komputerowy.

b) Pracownik zatrudniony przy przetwarzaniu danych osobowych przechowywanych w formie papierowej zobowiązany jest zawiadomić administratora bezpieczeństwa informacji o naruszeniu zbioru danych osobowych a w szczególności przy stwierdzeniu:
- częściowym lub całkowitym braku bazy danych
- kradzieży w pomieszczeniu w którym przechowywane były zbiory danych osobowych
- śladów prób włamania się do tego pomieszczenia
- częściowym lub całkowitym zniszczeniu zbioru na skutek przypadku losowego

c) Administrator Systemu Informatycznego, po otrzymaniu zawiadomienia o naruszeniu zabezpieczenia systemu informatycznego powinien niezwłocznie:
- powiadomić Administratora Danych i Administratora Bezpieczeństwa Informacji
- przeprowadzić postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia i osoby odpowiedzialnej za naruszenie,
- podjąć działania zabezpieczające system przed ponownym naruszeniem,
- sporządzić protokół dokonanych czynności.

d) W przypadku kradzieży z pomieszczenia, w którym znajdują się komputery należy niezwłocznie poinformować o tym fakcie policję.

9.Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Aktualny opis sposobu zarządzania systemem informatycznym służącym do przetwarzania danych osobowych znajduje się w załączniku 2 do zarządzenia Starosty Mławskiego w sprawie wprowadzenia polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Załącznik jest aktualizowany w przypadku wystąpienia potrzeby wprowadzeniu istotnych zmian w zakresie zarządzania systemem informatycznym. Podpisany jest przez Administratora Danych.

10.Ewidencja osób upoważnionych do przetwarzania danych osobowych

Ewidencja osób upoważnionych do przetwarzania danych osobowych prowadzona i aktualizowana jest przez Administratora Bezpieczeństwa Informacji nie rzadziej, niż co 3 miesiące.

STAROSTA
Włodzimierz A. Wojnarowski

Załącznik nr 2
do Zarządzenia nr 51/2011
Starosty Mławskiego
z dnia 1.12.2011

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:

1 egz. do kadr - celem umieszczenia teczce akt osobowych,
1 egz. do osoby której upoważnienie dotyczy,
1 egz. do teczki spraw o sygnaturze 142.3 (według JRWA)
1 egz. do ABI,

2. Administrator Bezpieczeństwa Informacji (ABI):
aktualizuje ewidencję osób upoważnionych do przetwarzania danych osobowych w systemie informatycznym na podstawie informacji pochodzących od pracownika kadr i Administratorów Systemu Informatycznego.

3. Administratorzy Systemu Informatycznego (ASI) tzn. upoważnieni pracownicy zatrudnieni w Starostwie Powiatowym w Mławie na etacie informatyka lub starszego informatyka:
a)rejestrują użytkownika w systemie i nadają mu określone uprawnienia oraz hasło
b)nadają identyfikator i prowadza ewidencję identyfikatorów użytkowników
c)umożliwiają użytkownikowi zastosowanie i zmianę hasła oraz przechowują hasła użytkowników wraz z ich comiesięcznymi aktualizacjami w zamkniętych kopertach
d)prowadzą rejestr komputerów, serwerów, ich dysków twardych oraz ich użytkowników

4. Użytkownik:
uwierzytelnia się w systemie po podaniu identyfikatora oraz hasła uzyskanego od Informatyka; użytkownik zmienia hasło na swoje, którego nie wolno przekazać nikomu innemu i rozpoczyna pracę w aplikacji. Nie rzadziej niż co 30 dni zmienia hasło i przekazuje w zamkniętej kopercie Administratorom Systemu Informacji.

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. Inspektor ds. kadr przekazuje do ABI informację pisemną o zatrudnieniu lub ustaniu zatrudnienia, zmianie zakresu obowiązków i utracie upoważnienia niezwłocznie 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:
   a) dostępu do sieci lokalnej,
   b) dostępu do aplikacji.
2. Do uwierzytelnienia użytkownika w systemie na obu poziomach stosuje się hasła.
3. Hasło dostępu da sieci lokalnej składa się, co. najmniej z 4 znaków, zawiera małe i wielkie litery oraz cyfry i znaki specjalne.
4. Hasła nie mogą być powszechnie używanymi sławami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
5. Hasła nie mogą być ujawniane nawet po utracie przez nie ważności.
6. Zmiana hasła da systemu następuje nie rzadziej, niż co 30 dni lub niezwłocznie w przypadku podejrzenia, że hasła mogły zostać ujawniane.
7. 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 poda właściwy identyfikator i hasło.
8. Identyfikator użytkownika jest wpisywany da ewidencji osób upoważnianych da przetwarzania danych osobowych w systemie informatycznym wraz z zakresem upoważnienia oraz datą nadania uprawnień.
9. Aplikacja powinna wymuszać na użytkowniku zmianę swojego, hasłą, co 30 dni.
10. System zostanie wyłączany po trzykrotnej próbie nieudanego, logowania się - uzależniane od ustawień BIOS-u.
11. Aplikacja zastanie wyłączana po trzykrotnej próbie nieudanego, logowania się
12. System zastanie wyłączany po określonym czasie logowania.
13. Użytkownik zapisuje swój identyfikator i hasła dostępu da aplikacji zarządzającej systemem administrowania i przekazuje je w kopercie ASI. Koperta zastaje zabezpieczana w sposób uniemożliwiający jej nieuważne otwarcie. ASI przechowuje kopertę w kasecie metalowej w pokoju informatyków.

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

a) przy każdorazowym opuszczeniu stanowiska komputerowego, dopilnować, aby na ekranie nie były wyświetlane dane osobowe,

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

3. Procedura zakończenia pracy w systemie

a) zarchiwizować dane,

b) zamknąć aplikację,

c) zamknąć system,

d) wyłączyć monitor i drukarkę.

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

1. W cyklu dziennym kopie wykonywane są przez ASI lub automatycznie przez system na serwerze, który pełni funkcję archiwum przy wykorzystaniu odrębnego stanowiska komputerowego.

2. W wyjątkowych przypadkach takich jak np. niebezpieczeństwo utraty danych kopie zapasowe mogą być wykonywane przez użytkowników aplikacji na zewnętrznych elektronicznych nośnikach informacji.

3. Administratorzy Systemu Informatycznego w sytuacji opisanej w pkt.2, sprawują nadzór nad wykonywaniem kopii zapasowych, weryfikuje ich poprawność. Kopie te przechowywane są w pomieszczeniu ASI w szafie.

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

1. Dane osobowe w postaci elektronicznej przetwarzane w systemie informatycznym, zapisane na dyskietkach, płytach CD i innych zewnętrznych (wymontowane dyski twarde, nośniki typu pendrive, karty elektroniczne i in.) lub wewnętrznych nośnikach (dyski zamontowane w komputerach, serwerach) nie mogą być wynoszone poza siedzibę urzędu.

2. Wewnętrzne elektroniczne nośniki informacji zamontowane na komputerach i serwerach jako dyski twarde są przechowywane w pomieszczeniu stanowiących obszar przetwarzania danych osobowych, określony w polityce bezpieczeństwa.

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

4. 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.

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

6. Kopie zapasowe zbioru danych osobowych są przechowywane w szafie w pokoju ASI.

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

1. Nadzór nad instalowaniem nowego oprogramowania antywirusowego oraz nad bieżącą jego aktualizacją sprawują Administratorzy Systemu Informatycznego (ASI).

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

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

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

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

6. O każdorazowym wykryciu wirusa przez oprogramowanie antywirusowe użytkownik obowiązany jest niezwłocznie poinformować ASI.

7. Po usunięciu wirusa ASI sprawdza system informatyczny oraz przywraca go do pełnej funkcjonalności i sprawności.

8. Administratorzy Systemu Informatycznego prowadzą rejestr przypadków zainfekowania komputerów i nośników wykorzystywanych do przetwarzania danych osobowych w systemie.

9. 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.

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

11. Ochrona systemu informatycznego używanego w starostwie polega na:
    a) ochronie przez identyfikator,
    b) ochronie za pomocą hasła,
    c) przydzielaniu praw,
    d) 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 z tego systemu w formie pisemnej .

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

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

3. Odnotowanie obejmuje informacje o:
    a) nazwie jednostki organizacyjnej lub imieniu i nazwisku osoby, której udostępniono dane,
    b) zakresie udostępnianych danych,
    c) 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 ASI.

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

1.Odpowiedzialni za przeglądy i konserwacje są ASI. O przeprowadzanych przeglądach i konserwacjach systemu informują ABI.

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 odpowiadają Administratorzy Systemu Informatycznego.

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

a) zmiany wersji oprogramowania serwera plików;
b) zmiany wersji oprogramowania stanowiska komputerowego użytkownika systemu;
c) zmiany systemu operacyjnego serwera plików;
d) zmiany systemu operacyjnego stanowisk komputerowego użytkownika systemu;
e) 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.

7.Sprawdzenie wymienione w pkt. 6 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 Administratorów Systemu Informatycznego.

9.Za prawidłowość przeprowadzenia przeglądów i konserwacji systemu odpowiadają Administratorzy 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 Danych oraz 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
- listy wszystkich komputerów Starostwa Powiatowego wraz z numeracja według symbolu K wraz z ich użytkownikami, parametrami technicznymi, numerami inwentarzowymi i numerami dysków twardych
- 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 przepisów o ochronie danych osobowych i zaleceń Administratora Bezpieczeństwa Informacji
h) zgłaszania Administratorowi Danych oraz Sekretarzowi Powiatu 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 za 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)realizację wymogu 30-dniowego okresu zmian haseł na komputerach użytkowników i przechowywanie ich w zamkniętych kopertach. Koperty z hasłami przechowywane są w kasetce pancernej w szafie pomieszczenia Administratorów Systemu Informacji.
e)procedury wykonywania kopii awaryjnych, określenie ich częstotliwości, zmianę nośników oraz ich właściwe przechowywanie, sprawdzanie poprawności zapisu i likwidację
f)lokalizację sprzętu komputerowego, ustawienie monitorów i drukarek uniemożliwiające wgląd w dane osobom nieupoważnionym lub kradzież wymiennych nośników danych
g) postępowania zgodnie z instrukcją w sytuacji naruszenia ochrony danych osobowych

STAROSTA
Włodzimierz A. Wojnarowski