Załącznik Nr 1 do zarządzenia
Wójta Gminy Męcinka
z dnia 4 lipca 2012roku

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMIE INFORMATYCZNYM URZĘDU GMINY MĘCINKA

§ 1.
Definicje

Ilekroć w niniejszym dokumencie jest mowa o:

1) urzędzie – należy przez to rozumieć Urząd Gminy Męcinka,

2) administratorze danych – należy przez to rozumieć osobę, o której mowa w Instrukcji przetwarzania danych osobowych,

3) administratorze bezpieczeństwa informacji – należy przez to rozumieć osobę, o której mowa w Instrukcji przetwarzania danych osobowych,

4) użytkowniku systemu – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym urzędu,

5) sieci lokalnej – należy przez to rozumieć połączenie systemów informatycznych urzędu wyłącznie dla własnych jej potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych,

6) instrukcji – Instrukcję zarządzania systemem informatycznym Urzędu Gminy Męcinka,

7) wójcie gminy – oznacza to Wójta Gminy Męcinka.

§ 2.
Obszar przetwarzania danych osobowych

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe stanowi załącznik Nr 2 do niniejszego opracowania.

§ 3.
Wykaz zbiorów danych osobowych przetwarzanych w systemie informatycznym

1. W skład systemu wchodzą:
   1) dokumentacja papierowa (korespondencja, wnioski, deklaracje, itd.),
   2) urządzenia i oprogramowanie komputerowe służące do przetwarzania informacji oraz procedury przetwarzania danych w tym systemie, w tym procedury awaryjne,
   3) wydruki komputerowe.

2. Wykaz zbiorów danych osobowych przetwarzanych w systemie informatycznym stanowi załącznik Nr 2 do niniejszego opracowania.

§ 4.
Struktura zbioru danych osobowych

Opis struktury zbiorów danych osobowych oraz powiązania między zbiorami stanowi załącznik Nr 3 do niniejszego opracowania.

§ 5.
Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Środki ochrony fizycznej:

   1) okna w pomieszczeniach na parterze budynku urzędu są okratowane a cały budynek zabezpieczony systemem alarmowym monitorowanym przez operatora zewnętrznego,
   2) urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach biurowych zabezpieczonych zamkami patentowymi,
   3) przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osoby zatrudnionej przy przetwarzaniu danych,
   4) pomieszczenia, o których mowa w punkcie 3, zamykane są na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich,
   5) w przypadku przebywania osób postronnych w pomieszczeniach, o których mowa w punkcie 3, monitory stanowisk dostępu do danych osobowych ustawione są w taki sposób, aby uniemożliwić tym osobom wgląd w dane,
   6) do przebywania w pomieszczeniach serwera (pokój nr 18) uprawnieni są: administrator danych, administrator bezpieczeństwa informacji, inne osoby upoważnione przez wójta gminy,
   7) przebywanie w pomieszczeniu serwera osób nieuprawnionych (konserwator, elektryk, sprzątaczka) dopuszczalne jest tylko w obecności jednej z osób wymienionych lub upoważnionych, o których mowa w pkt 6.

2. Środki sprzętowe, informatyczne i telekomunikacyjne:

1) zastosowano sprzętowe niszczarki dokumentów papierowych,
2) serwery wchodzące w skład systemu informatycznego posiadają indywidualne zasilanie awaryjne UPS zapobiegające skutkom nagłych zaników napięcia,
3) zastosowano sieć lokalną (Ethernet) w typologii gwiazdy,
4) na serwerze zainstalowano oprogramowanie firewall zabezpieczające przed atakiem z zewnątrz,
5) na serwerze oraz w poszczególnych stacjach roboczych zainstalowano oprogramowanie antywirusowe; poczta elektroniczna wpływająca do urzędu skanowana jest programem antywirusowym przed przesłaniem jej do użytkownika,
6) kopie awaryjne baz danych wykonywane są:
    a) w cyklu dziennym (na dysk twardy),
    b) w cyklu tygodniowym (na nośnik optyczny – płyta CD).

3. Środki ochrony w ramach oprogramowania systemów:

1) w systemie informatycznym zdefiniowane zostały prawa dostępu do zasobów informatycznych oparte o unikalny identyfikator i hasło,
2) dostęp fizyczny do baz danych osobowych zastrzeżony jest wyłącznie dla administratora bezpieczeństwa informacji, a w czasie jego nieobecności dla innej osoby wskazanej przez wójta gminy,
3) konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych jedynie za pośrednictwem aplikacji,
4) wszystkie stacje robocze chronione są przez program antywirusowy,
5) w sieciowym systemie operacyjnym zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do sieci.

4. Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych:

1) zastosowano bazy danych w formacie DBF,MS ACCESS oraz MS SQL,BTRIVE,
2) fizyczny dostęp do baz danych jest zabezpieczony hasłem,
3) zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (unikalny identyfikator i hasło).

5. 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 wejściowym do systemu operacyjnego oraz hasłem do każdej aplikacji, w której przetwarzane są dane osobowe.

6. Środki organizacyjne:
1) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych oraz ich uprawnień,
2) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane są do zachowania ich w tajemnicy, na podstawie pisemnego zobowiązania,
3) osoby upoważnione do przetwarzania danych osobowych są przed dopuszczeniem ich do tych danych szkolone w zakresie obowiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych w systemie informatycznym,

4) wprowadzono instrukcję zarządzania systemem informatycznym,
5) zdefiniowano procedury postępowania w sytuacji naruszenia ochrony danych osobowych i określono je w Instrukcji,
6) określono sposób postępowania z nośnikami informacji.

ZAŁĄCZNIK NR 1
DO POLITYKI BEZPIECZEŃSTWA
PRZETWARZANIA DANYCH
OSOBOWYCH SYSTEMU
INFORMATYCZNEGO

WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

1. Przetwarzanie danych osobowych odbywa się w siedzibie urzędu zajmującego budynek nr 11 w Męcince.
   Pomieszczenia biurowe zajmują dwie kondygnacje, a przechowywanie i przetwarzanie danych osobowych w systemie informatycznym odbywa się:
   a) na I kondygnacji – parter – w pokoju Nr 8
   b) na II kondygnacji – I piętro – w pokojach:11,14,15,16,17,18 (serwer),21,22,23,24,26.

2. Przetwarzanie danych osobowych odbywa się wyłącznie z użyciem stacjonarnego sprzętu komputerowego.

3. Dokumentację papierową zawierającą dane osobowe przechowuje się w zamkniętych na zamki patentowe szafach biurowych.

4. Zapasowe kopie danych gromadzonych na płytach CD-R przechowuje się w szafie metalowej zlokalizowanej w pokoju Nr 18.

ZAŁĄCZNIK NR 2
DO POLITYKI BEZPIECZEŃSTWA
PRZETWARZANIA DANYCH
OSOBOWYCH SYSTEMU
INFORMATYCZNEGO

WYKAZ ZBIORÓW DANYCH OSOBOWYCH PRZETWARZANYCH W SYSTEMIE INFORMATYCZNYM

Lp.	Numer pokoju/ kondygnacja	Typ komputera, w którym przetwarzany jest zbiór danych	Nazwa zbioru/ nazwa stosowanego oprogramowania
1.	7/pierwsza	stacjonarny	1. EWIDENCJA NAJEMCÓW LOKALI KOMUNALNYCH (czynsze) 2. EWIDENCJA ODBIORCÓW WODY Z WODOCIĄGU GMINNEGO (Woda)
2.	11/druga	stacjonarny	EWIDENCJA PRACOWNIKÓW ZATRUDNIONYCH W URZĘDZIE GMINY
3.	26/druga	stacjonarny	SYSTEM INFORMACJI OŚWIATOWEJ
4.	22/druga	stacjonarny	1. EWIDENCJA PODATNIKÓW 2. EGZEKUCJA NALEŻNOŚCI GMINNYCH 3. KARTOTEKI ZALEGŁOŚCI CZYNSZOWYCH, DZIERŻAWNYCH I INNYCH DOCHODÓW GMINY 4. REJESTR PODATNIKÓW PODATKU OD ŚRODKÓW TRANSPORTOWYCH 5. KARTOTEKA UBEZPIECZONYCH ROLNIKÓW
5.	23/druga	stacjonarny	EWIDENCJA WYNAGRODZEŃ PRACOWNIKÓW ZATRUDNIONYCH W URZEDZIE GMINY
6.	24/druga	stacjonarny	1. EWIDENCJA LUDNOŚCI I DOWODÓW OSOBISTYCH (Ewid) 2. REJESTR POBOROWYCH
7.	24/druga	stacjonarny	EWIDENCJA DZIAŁALNOŚCI GOSPODARCZEJ(CEIDG)
8.	24/druga	stacjonarny	SYSTEM WYDAWANIA DOWODÓW OSOBISTYCH

ZAŁĄCZNIK NR 3 DO POLITYKI
BEZPIECZEŃSTWA
PRZETWARZANIA DANYCH
OSOBOWYCH SYSTEMU
INFORMATYCZNEGO

STRUKTURA ZBIORÓW DANYCH OSOBOWYCH I SPOSÓB PRZEPŁYWU DANYCH

1. Baza danych ewidencji ludności – dane osobowe przetwarzane są w wyłącznie przez program EWID w celu prowadzenia ewidencji.
2. Baza danych podatków – rolny/leśny, od nieruchomości, od osób prawnych i fizycznych – dane przetwarzane są przy użyciu bazy danych przez programy APAS oraz APUP3. Dane z programu APUP3 eksportowane są do postaci pliku o formacie akceptowanym przez program TYT-DRUK w celu wydruku tytułów wykonawczych.
3. Płace pracowników urzędu i instytucji kultury – dane przetwarzane są w postaci plików dbf w programie PŁACE, istnieje możliwość przepływu (tylko odczyt) danych osobowych z programu KADRY. Z programu PŁACE dane osobowe eksportowane są do postaci pliku (.kdu) ustalonym przez twórców programu PŁATNIK. Plik ten jest importowany do programu PŁATNIK, który służy do rozliczeń pracowników z ZUS.
4. Program PŁATNIK – struktury danych osobowych, program wykorzystuje transmisje danych poprzez sieć publiczną sposobem, jaki określił Zakład Ubezpieczeń Społecznych.
5. Baza danych osobowych odbiorców wody – dane przetwarzane są w postaci plików dbf wyłącznie przez program WODA, istnieje możliwość eksportu danych osobowych do przenośnego komputera PSION umożliwiającego rejestrację i przechowywanie danych w terenie oraz ponownego ich importu.
6. Baza danych osobowych najemców lokali komunalnych – dane przetwarzane są w postaci plików dbf wyłącznie przez program CZYNSZE.