Załącznik Nr 1
do Zarządzenia Nr 39
Wójta Gminy Secemin
z dnia 30 sierpnia 2012 roku

Polityka Bezpieczeństwa Informacji (PBI)

URZĄDU GMINY SECEMIN

Załączniki :

1. Instrukcja zarządzania systemem informatycznym
2. Wykaz pomieszczeń
3. Wykaz zbiorów
4. Wzór upoważnienia
5. Wzór oświadczenia
6. Ewidencja osób
7. Wzór potwierdzenia

I CEL PRZYGOTOWANIA POLITYKI BEZPIECZEŃSTWA

Podstawowym celem przyświecającym przygotowaniu i wdrożeniu dokumentu Polityki Bezpieczeństwa było zapewnienie zgodności działania Urzędu Gminy Secemin z ustawą o ochronie danych osobowych oraz jej rozporządzeniami wykonawczymi. Opracowany dokument Polityki Bezpieczeństwa został w oparciu o wytyczne zawarte w następujących aktach prawnych:

1) 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. z 2004 r., Nr 100, poz. 1024 z późn. zm.),

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

3) ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (tj. Dz.U. z 2001 r. nr 128, poz. 1402 z późn. zm.).

Należy przez powyższe rozumieć w szczególności realizację w niniejszym dokumencie wymogu opisania sposobu przetwarzania danych osobowych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. Zadaniem Polityki Bezpieczeństwa jest także określenie podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych oraz wymagań w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych.

Polityka bezpieczeństwa przetwarzania danych osobowych zwana dalej „Polityką bezpieczeństwa", określa podstawowe zasady dotyczące zapewnienia bezpieczeństwa w zakresie danych osobowych przetwarzanych w zbiorach danych:

1) tradycyjnych, w szczególności kartotekach, księgach, skorowidzach, aktach osobowych, wykazach, w zbiorach ewidencyjnych;

2) w systemach informatycznych, w szczególności deklaracje ZUS, ewidencje płacowe, informacje skarbowe, ewidencje statystyczne, plany organizacyjne.

3) w systemach informatycznych, ewidencja mieszkańców, ewidencja małżeństw i zgonów.

Ilekroć w Polityce Bezpieczeństwa jest mowa o:

1) *ustawie* – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych z dnia 29 sierpnia 1997r. (tekst jedn. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.);

2) *administrator danych osobowych* – rozumie się Wójta Gminy Secemin

3) administrator bezpieczeństwa informacji – rozumie się Sekretarza Gminy Secemin

4) *administrator sieci* – rozumie się osobę odpowiedzialną za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych, służących do przetwarzania danych osobowych;

6) *nośniki danych osobowych* – dyskietki, płyty CD lub DVD, pamięć flash, dyski twarde, taśmy magnetyczne lub inne urządzenia/ materiały służące do przechowywania plików z danymi;

7) *osoba upoważniona (użytkownik)* – osoba posiadająca upoważnienie wydane przez administratora danych osobowych ;

8) *dane osobowe* - w rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;

9) *przetwarzanie danych* - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;

10) *zbiór danych* - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów;

11) *system informatyczny* - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

12) *identyfikator użytkownika (login*) - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

13) *hasło* - ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

14) *uwierzytelnianie* — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

15) *poufności danych* — rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.

16) *PBI* – Polityka Bezpieczeństwa Informacji

17) *ADO* – Administrator Danych Osobowych

18) *ABI* – Administrator Bezpieczeństwa Informacji

II POSTANOWIENIA OGÓLNE

Wójt Gminy Secemin, świadomy wagi problemów związanych z ochroną prawa do prywatności, w tym w szczególności osób fizycznych powierzających Urzędowi Gminy swoje dane osobowe, do właściwej i skutecznej ochrony tych danych deklaruje zamiar:

1. Podejmowania wszystkich działań niezbędnych dla ochrony praw i usprawiedliwionych interesów jednostki związanych z bezpieczeństwem danych osobowych,

2. Stałego podnoszenia świadomości oraz kwalifikacji osób przetwarzających dane osobowe w UG w zakresie problematyki bezpieczeństwa tych danych, w tym propagowania świadomości wartości powierzonych danych osobowych jako czynnika wpływającego na jakość i ciągłość działalności oraz wiarygodność UG.

3. Traktowania obowiązków osób zatrudnionych przy przetwarzaniu danych osobowych jako należących do kategorii podstawowych obowiązków pracowniczych oraz stanowczego egzekwowania ich wykonania przez zatrudnione osoby,

4. Doskonalenia i rozwijania nowoczesnych metod zabezpieczenia danych przed zagrożeniami związanymi z ich przetwarzaniem, szczególnie w zakresie dotyczącym dynamicznego rozwoju metod i technik przetwarzania tych danych w systemach informatycznych oraz sieciach telekomunikacyjnych.

Realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych Urząd Gminy dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:

1. przetwarzane zgodnie z prawem,
2. zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
3. merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
4. przechowywane w postaci umożliwiającej identyfikacje osób, których dotyczą, nie dłużej jednak niż jest to niezbędne do osiągnięcia celu przetwarzania.

W celu zabezpieczenia danych osobowych przed nieuprawnionym udostępnieniem Administrator wprowadza określone niniejszym dokumentem zasady przetwarzania danych. Zasady te określa w szczególności polityka bezpieczeństwa oraz instrukcje stanowiące załączniki do polityki bezpieczeństwa tj. instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych – załącznik nr 1 do Polityki Bezpieczeństwa Informacji.

Mając świadomość, iż żadne zabezpieczenie techniczne nie gwarantuje 100%-towej szczelności systemu, konieczne jest, aby każdy pracownik upoważniony do przetwarzania danych pełen świadomej odpowiedzialności, postępował zgodnie z przyjętymi zasadami i minimalizował zagrożenia wynikające z błędów ludzkich.
Zasady, działania, kompetencje i zakresy odpowiedzialności opisane w dokumentach Polityki Bezpieczeństwa Informacji obowiązują wszystkich pracowników Urzędu.

Ponadto w trosce o czytelny i uporządkowany stan materii, wprowadza się stosowne środki organizacyjne i techniczne zapewniające właściwą ochronę danych oraz nakazuje ich bezwzględne stosowanie, zwłaszcza przez osoby dopuszczone do przetwarzania danych.

Polityka Bezpieczeństwa Informacji będzie weryfikowana i dostosowywana w celu zapewnienia odpowiedniego poziomu bezpieczeństwa. Przeglądy dokumentacji polityki bezpieczeństwa będą odbywać się nie rzadziej niż raz w roku.

II CHARAKTERYSTYKA INSTYTUCJI

1. Urząd Gminy Secemin prowadzi obsługę mieszkańców gminy Secemin, ustala i pobiera podatki rolne, od środków transportowych, od nieruchomości, zapewnia dostęp mieszkańcom do informacji dotyczącej nieruchomości, ustala i nadaje nr porządkowe działkom, prowadzi ewidencję mieszkańców, wyborców, a także ewidencjonuje i wydaje akta małżeństwa, zgonu, nadaje nr PESEL i wydaje dowody osobiste.
2. Obszar fizyczny przetwarzania danych obejmuje siedzibę Urzędu Gminy zlokalizowany w budynku przy ul. Struga 2 w Seceminie.

Szczegółowy wykaz pomieszczeń stanowi załącznik nr 2 do niniejszej dokumentacji.

III CELE BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Pod pojęciem bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy należy rozumieć zdolność Urzędu do ochrony danych osobowych przetwarzanych w tych systemach, przed zagrożeniami, które mogą wykorzystać ich podatność i doprowadzić do:
   a. udostępnienia lub ujawnienia danych osobowych nieupoważnionym podmiotom,
   b. zmiany lub zniszczenia danych w sposób nieautoryzowany.

Ogólnym celem prowadzonej w Urzędzie Gminy polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych jest określenie poziomu bezpieczeństwa przetwarzania danych osobowych w poszczególnych systemach informatycznych eksploatowanych w Urzędzie oraz określenie dla tych systemów wymagań bezpieczeństwa w zakresie środków technicznych i organizacyjnych, które powinny być odpowiednie do zagrożeń oraz kategorii danych objętych ochroną.

Problemy związane z wyznaczaniem szczegółowych celów bezpieczeństwa są formułowane i rozwiązywane przy założeniu, że:

1. Poziom bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie wyznaczają:
   a. ryzyko udostępnienia lub ujawnienia przetwarzanych danych osobowych nieupoważnionym podmiotom,
   b. ryzyko zmiany lub zniszczenia danych w sposób nieautoryzowany.

2. O poufności i integralności danych osobowych przetwarzanych w systemach informatycznych decyduje sprawność i niezawodność tych systemów oraz zabezpieczenie ich zasobów.

3. Szczegółowe cele bezpieczeństwa wyznacza się odrębnie dla każdego systemu informatycznego, biorąc pod uwagę kategorię danych przetwarzanych w systemie i zagrożenia oraz wymagania bezpieczeństwa określone w przepisach o ochronie danych osobowych.

IV WYKAZ ZBIORÓW

1. Dane osobowe gromadzone są w zbiorach.

2. Wykaz zbiorów danych osobowych stanowi załącznik nr 3

V ŚRODKI ORGANIZACYJNE OCHRONY DANYCH OSOBOWYCH

1. W celu stworzenia właściwych zabezpieczeń, które powinny bezpośrednio oddziaływać na procesy przetwarzania danych, wprowadza się następujące środki organizacyjne:

- Przetwarzanie danych osobowych w Urzędzie Gminy może odbywać się wyłącznie w ramach wykonywania zadań służbowych. Zakres uprawnień wynika z zakresu tych zadań.
- Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne upoważnienie. Wzór upoważnienia stanowi załącznik nr 4 do niniejszej dokumentacji.
- Każdy pracownik podpisuje również OŚWIADCZENIE zachowaniu poufności i zapoznaniu się z przepisami wzór załącznik nr 5
- Ewidencja osób, które mają dostęp do zbiorów danych osobowych stanowi załącznik nr 6
- Każdy pracownik Urzędu Gminy musi odbyć szkolenie z zakresu ochrony danych osobowych. Za organizację szkoleń odpowiedzialny jest administrator bezpieczeństwa informacji (ABI)
- Nowo przyjęty pracownik, stażysta, uczeń będący na praktykach odbywa szkolenie z zakresu polityki bezpieczeństwa przed przystąpieniem do przetwarzania danych.
- Ponadto każdy upoważniony do przetwarzania danych potwierdza pisemnie fakt zapoznania się z niniejszą dokumentacją i zrozumieniem wszystkich zasad bezpieczeństwa. Wzór potwierdzenia stanowi załącznik nr 7 do niniejszej dokumentacji.
- Obszar przetwarzania danych osobowych określony w załączniku nr 2 do niniejszej dokumentacji, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych
- Pomieszczenia stanowiące obszar przetwarzania danych są zamykane na klucz. Każdy pracownik pobiera i zdaje klucze na sekretariacie, gdzie są one przechowywane w zamkniętej szafce.
- Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
- Przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna oraz usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w odpowiednich zamykanych szafach lub biurkach.

VI. ODPOWIEDZIALNOŚĆ ZA REALIZACJĘ POLITYKI BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Odpowiedzialność za ochronę danych osobowych w Urzędzie ponoszą wszyscy pracownicy urzędu, w zakresie odpowiednim do nałożonych na nich obowiązków oraz posiadanych przez nich kompetencji.

Wójt Gminy ponosi odpowiedzialność za stworzenie odpowiednich warunków prawnych, organizacyjnych i finansowych do wdrożenia systemu ochrony danych osobowych przetwarzanych w systemach informatycznych, a szczególności odpowiada za:

l/ stworzenie w Urzędzie Gminy odpowiedniej struktury organizacyjnej ze stanowiskami przeznaczonymi dla osób odpowiedzialnych za zarządzanie bezpieczeństwem informacji,

2/ określenie kompetencji i odpowiedzialności kierowników poszczególnych komórek organizacyjnych dotyczących wykonywania zadań wynikających z przepisów o ochronie danych osobowych oraz mających związek z funkcjonowaniem systemu ochrony,

3/ zgłoszenie do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbiorów danych osobowych przetwarzanych w Urzędzie Gminy, zgodnie z art. 41 ustawy o ochronie danych osobowych,

4/ wprowadzenie do użytku w Urzędzie Gminy:

a) Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych,

b) Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych

Sporządził
Administrator Bezpieczeństwa Informacji

……..

Zatwierdził:
Administrator Danych Osobowych

……..

HISTORIA DOKUMENTU

Wersja	Data wersji	Opis	Rozdziały**	Autorzy	Zatwierdził
1.01	01.07.2012	[…]	[…]	[…]	[…]

* Np. utworzenie nowego dokumentu, modyfikacja, weryfikacja, uzupełnienie.
** Wymienić rozdziały, w których dokonano zmian.