Załącznik Nr 1
do Zarządzenia Wójta Gminy
Nr 28/OR/09 z dnia 20.04.2009r

POLITYKA BEZPIECZEŃSTWA

Urząd Gminy w Łodygowicach

Część ogólna

Nadrzędną rolą w działaniach Wójta Gminy wynikających z jego funkcji jest ochrona powierzonych danych osobowych. Odpowiedzialność za powierzone dane osobowe ponoszą wszyscy pracownicy Urzędu Gminy w Łodygowicach, mający dostęp do danych osobowych w ramach swych obowiązków służbowych (art. 1 ust. 1 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych. „Dane osobowe" są to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny (np. PEESEL, NIP) albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne (zgodnie z art. 6 ust. 1 i ust. 2 ustawy)
„Polityka bezpieczeństwa" jest to zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji zasobów danych osobowych.
Celem „Polityki bezpieczeństwa" jest przyjęcie, wdrożenie i realizacja takich działań przy wykorzystaniu środków technicznych i organizacyjnych, które zapewnią maksymalny poziom bezpieczeństwa procesu przetwarzania danych osobowych, chroniąc je przed nieautoryzowanym dostępem, utrata poufności, nieuprawniona modyfikacja oraz zachowaniu ich integralności i rozliczalności.
„Polityka bezpieczeństwa" opisuje działania, które w jak najbardziej efektywny sposób pozwolą osiągnąć postawiony cel.
W celu zapewnienia bezpieczeństwa przetwarzanych danych wymaga się, aby wszyscy jego użytkownicy byli świadomi konieczności ochrony wykorzystywanych zasobów. Konsekwencja nie stosowania przez pracownika środków bezpieczeństwa określonych w instrukcjach wewnętrznych może być zniszczenie części lub całości systemów informatycznych, utrata poufności, autentyczności, straty finansowe, jak również utrata wizerunku.

Pracownicy są odpowiedzialni za bezpieczeństwo danych, do których maja dostęp. W szczególności w systemach informatycznych odpowiadają oni za poprawne wprowadzanie informacji do tych systemów oraz za użycie, zniszczenie lub uszkodzenie sprzętu oraz znajdujących się na nim danych i oprogramowania.

Zarządzanie bezpieczeństwem zasobów danych osobowych stanowi proces ciągły, na który składają się takie elementy, jak: identyfikacja oraz analiza zagrożeń i ryzyka, stosowanie odpowiednich zabezpieczeń, monitorowanie wdrażania i eksploatacji zabezpieczeń, wykrywanie i reagowanie na incydenty.

Część Szczegółowa

I. Dane osobowe gromadzone są przez Urząd Gminy w Łodygowicach w systemach informatycznych, na zewnętrznych nośnikach danych oraz w zbiorach manualnych. Rozwiązania techniczne w systemach informatycznych pozwalają na uzupełnianie tych samych danych z innych posiadanych zasobów w ramach jednostki, co przekłada się na ich efektywniejsze wykorzystanie w załatwianiu spraw. Zakres gromadzonych danych osobowych jest zgodny z przepisami prawa.

II. Sposób przepływu danych pomiędzy systemami.

Gromadzenie danych następuje przez pozyskiwanie ich z danych źródłowych, a także z innych zasobów. Gromadzone dane osobowe są udostępniane pracownikom w zakresie niezbędnym do ich pracy i wynikającym z przepisów prawa poprzez posiadane systemy informatyczne. Dane udostępniane są poprzez moduły do przeglądania danych, np. przeglądarki, zewnętrzny plik wymiany lub przy wykorzystaniu specjalnych mechanizmów baz danych. Możliwość wglądu przez pracowników w dane osobowe pozwala na ich porównywanie i sprostowanie ewentualnych rozbieżności ograniczając jednocześnie ilość wyjaśnień.

III. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Urząd Gminy w Łodygowicach przetwarza dane osobowe na podstawie przepisów prawa. Dane osobowe mogą być udostępnianie zgodnie z art. 29 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

Charakter oraz ilość przetwarzanych danych, powoduje konieczność ich ochrony przed nieautoryzowanym dostępem, utratą poufności, nieuprawnioną modyfikacją. Podejmowane są działania służące zachowaniu ich integralności i rozliczalności. W celu zapewnienia ochrony danych osobowych stosuje się odpowiednie rozwiązania organizacyjne i techniczne:

1. Budynek Urzędu Gminy objęty jest systemem kontroli dostępu, w tym sygnalizacji włamania.
2. Elektroniczne systemy monitoringu pozwalają na kontrolę ruchu osób i informują firmę ochraniającą budynek o przypadkach nieautoryzowanego wejścia.
3. Każdy pracownik Urzędu Gminy przed dopuszczeniem do przetwarzania danych osobowych zobowiązany jest do zapoznania się oraz stosowania przepisów ustawy o ochronie danych osobowych.

IV. Postępowanie w zakresie komunikacji w sieci komputerowej.

1. Podłączenie sprzętu komputerowego do sieci teleinformatycznej wykonuje Administrator Systemu na polecenie Wójta Gminy lub przez niego upoważnionego pracownika.
2. Zasoby informatyczne mogą być wykorzystywane tylko do wykonywania obowiązków służbowych.
3. Komunikacja pomiędzy pracownikami następuje poprzez pocztę elektroniczną oraz katalogi udostępnione w sieci.

V. Zakres obowiązków Administratora Bezpieczeństwa Informacji.

1. Analizuje, czy zakres przetwarzanych danych osobowych w jednostce jest adekwatny do potrzeb i jest zgodny z ustawą o ochronie danych osobowych.
2. Odpowiada za zastosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.
3. Opracowuje druk upoważnienia dopuszczającego do obsługi systemów informatycznych służących do przetwarzania danych osobowych.
4. Prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych.
5. Zgłasza do GIODO wszelkie zmiany w zbiorach danych osobowych uprzednio zgłoszonych.
6. Zgłasza do GIODO nowe zbiory osób dotychczas niezgłoszonych, a podlegających zgłoszeniu.
7. Zapewnia kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.
8. Opracowuje i przechowuje dokumentację służącą do ochrony przetwarzanych danych osobowych, w skład której wchodzą: polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym.
9. Uwzględniając kategorie przetwarzanych danych osobowych oraz zagrożenia, wprowadza poziomy bezpieczeństwa przetwarzanych danych w systemie informatycznym.

VI. Wykaz pomieszczeń, w których przetwarzane są dane osobowe.

1. pokoje nr 27,28 – Urząd Stanu Cywilnego,
2. pokój nr 23 – Referat Finansowy (podatki),
3. pokoje nr 24, 25 – Referat Finansowy (płace i ZUS),
4. pokój nr 29 – Referat Organizacyjny (ewidencja działalności gospodarczej),
5. pokój nr 30 – Referat Organizacyjny (kadry),
6. pokoje nr 14,15,18 – Referat Rozwoju Inwestycji i Promocji
7. pokój nr 9 – Kasa Urzędu Gminy
8. Biuro Obsługi Klienta