**ZARZĄDZENIE NR 0050.117.2011**

**WÓJTA GMINY KRZYŻANOWICE – KIEROWNIKA URZĘDU GMINY**

**z dnia 15.11.2011 roku.**

**w sprawie** : wprowadzenia Polityki Bezpieczeństwa w Urzędzie Gminy Krzyżanowice

**Na podstawie:**

1) art. 33 ust. 3 ustawy z dnia 8 marca 1990 o samorządzie gminnym (tekst jedn. z 2001 r. Dz. U. Nr 142 poz. 1591 z późn. zm.)
2) art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. z 2002 r. Dz. U. Nr 101 poz. 926 z późn. zm.) w związku z §3 ust. 1 rozporządzenia 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. Nr 100 poz. 1024)

**zarządzam, co następuje :**

§ 1.

1. Wprowadzam Politykę Bezpieczeństwa celem zapewnienia bezpieczeństwa przetwarzanych danych osobowych.

2. Polityka Bezpieczeństwa zawiera zbiór procedur i zasad dotyczących przetwarzania danych osobowych.

§ 2

Ilekroć w Polityce Bezpieczeństwa jest mowa o:

1) ustawie - rozumie sie przez to ustawę z 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. z 2002 r. Dz.U. Nr 101, poz. 926 ze zm.);
2) rozporządzeniu - rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 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. Nr 100, poz. 1024);
3) Administratorze Danych - rozumie się przez to Gminę Krzyżanowice reprezentowaną przez Wójta Gminy Krzyżanowice,
4) Administratorze Bezpieczeństwa Informacji - rozumie się pracownika, który nadzoruje przestrzeganie zasady ochrony danych osobowych, o których mowa w art. 36 ust. 1 ustawy,

5) Administratorze Systemów Informatycznych – rozumie się informatyka zatrudnionego w Urzędzie Gminy Krzyżanowice w ramach umowy o pracę lub umowy cywilnoprawnej.
6) osobie upoważnionej do przetwarzania danych osobowych - rozumie się przez to osobę zatrudnioną na podstawie umowy o pracę, umowy zlecenia lub innej umowy oraz osobę odbywającą staż absolwencki lub praktykę studencką, którą Administrator Danych upoważnił do przetwarzania danych osobowych,
7) przetwarzaniu 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,
8) systemie informatycznym Administratora Danych - rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów procedur przetwarzania informacji i narzędzi programowych,
9) serwerze – rozumie się przez to komputer umieszczony w serwerowni, udostępniający dane w sieci informatycznej Urzędu Gminy,
10) serwerownia – rozumie się przez to pomieszczenie zlokalizowane na parterze w budynku Urzędu Gminy,
11) Instrukcji Zarządzania Systemem Informatycznym to instrukcja stanowiąca integralną część Polityki Bezpieczeństwa,
12) Instrukcji kancelaryjnej - rozumie się przez to rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011r. w sprawie instrukcji kancelaryjnej jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych ( Dz. U. Nr 14 poz. 67 z późn. zm.),

**§ 3**

Stosownie do § 6 ust. 1 pkt. 3 rozporządzenia, po uwzględnieniu kategorii przetwarzanych danych osobowych oraz zagrożenia ich bezpieczeństwa wprowadza się wysoki poziom bezpieczeństwa przetwarzanych danych osobowych w systemie informatycznym Administratora Danych.

**§ 4**

Polityka Bezpieczeństwa ma zastosowanie do przetwarzania danych osobowych:
1) w sposób tradycyjny - w księgach, wykazach i innych zbiorach ewidencyjnych,
2) w systemach informatycznych.

**§ 5**

Czynności przetwarzania danych osobowych może wykonywać wyłącznie:
1) osoba upoważniona do przetwarzania danych osobowych,
2) podmiot, któremu na podstawie art. 31 ustawy powierzono przetwarzanie danych osobowych poprzez zawarcie stosownej umowy.

**§ 6**

1. Administrator Danych realizuje następujące zadania:
1) podejmuje decyzje o celach i środkach przetwarzania danych osobowych, z uwzględnieniem przepisów obowiązującego prawa,
2) stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną
3) upoważnia osoby do przetwarzania danych osobowych.
Wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 1 do niniejszego Zarządzenia.

4) wyznacza Administratora Bezpieczeństwa Informacji, podejmuje działania w przypadku naruszenia lub podejrzenia naruszenia procedur Polityki Bezpieczeństwa w Urzędzie Gminy Krzyżanowice – dalej Polityki Bezpieczeństwa.

2. Administrator Bezpieczeństwa Informacji przy współudziale Administratora Systemów Informatycznych realizuje następujące zadania:
1) prowadzi oraz aktualizuje dokumentację opisującą sposób przetwarzania danych osobowych,
2) zarządza systemem informatycznym Administratora Danych posługując się hasłem dostępu do wszystkich serwerów i stacji roboczych z pozycji administratora,
3) na wniosek Administratora Danych dokonuje:
   a) rejestracji i wyrejestrowania użytkownika w systemie informatycznym Administratora Danych,
   b) zmiany identyfikatora użytkownika,
4) nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych oraz systemów informatycznych,
5) aktualizuje oprogramowanie antywirusowe oraz określa częstotliwość automatycznych aktualizacji definicji wirusów dokonywanych przez to oprogramowanie,
6) prowadzi ewidencję stanowisk komputerowych i osób odpowiedzialnych za ich użytkowanie,
7) podejmuje działania w razie wykrycia naruszeń w systemie informatycznym Administratora Danych,
8) prowadzi dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym Administratora Danych,
9) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje o tym Administratora Danych i współdziała z nim przy jego usuwaniu,
10) nadzoruje wykonywanie napraw, konserwacji oraz likwidacji urządzeń komputerowych, na których zapisane są dane osobowe,
11) podejmuje działania służące zapewnieniu:
   a) niezawodności zasilania komputerów i innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
   b) bezpiecznej wymiany danych w sieci wewnętrznej.

3. Administrator Bezpieczeństwa Informacji realizuje następujące zadania:
1) przygotowuje upoważnienia do przetwarzania danych osobowych,
2) prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych,
3) przygotowuje wnioski zgłoszeń rejestracyjnych i aktualizacyjnych zbiorów danych oraz wnioski o wykreślenie zbioru danych osobowych z Rejestru Zbiorów Danych Osobowych prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych,
4) aktualizuje w oparciu o zgłoszenia kierowników jednostek organizacyjnych Urzędu załącznik nr 4 do niniejszego Zarządzenia.
5) aktualizuje według potrzeb politykę bezpieczeństwa oraz instrukcję zarządzania systemem informatycznym
6) występuje z wnioskiem o udzielenie, zmianę oraz cofnięcie osobie upoważnienia do przetwarzania danych osobowych oraz o nadanie, czasowe zablokowanie oraz usunięcie identyfikatora i hasła dostępu do systemu informatycznego, którego wzór stanowi załącznik nr 2 do niniejszego Zarządzenia.
7) wprowadza i nadzoruje realizację obowiązków w zakresie fizycznego zabezpieczenia dokumentów, urządzeń i nośników zawierających dane osobowe,

1) wprowadza i kontroluje stosowanie fizycznych zabezpieczeń przetwarzania danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy, uszkodzeniem lub zniszczeniem,
2) prowadzi szkolenia osób upoważnionych do przetwarzania danych w zakresie:
   a) stosowania przepisów i instrukcji dotyczących ochrony danych osobowych,
   b) obowiązku sporządzania i przechowywania ich kopii, niszczenia wydruków i zapisów na nośnikach,
   c) sposobów ochrony danych przed osobami nieupoważnionymi,
   d) obowiązujących procedur udostępniania danych osobowych.
3) zgłasza osobie wykonującej zadania określone w ust. 3:
   a) konieczność zgłoszenia do rejestracji zbioru danych osobowych, dokonanie zmian w zbiorze lub jego wykreślenia,
   b) zmiany w zakresie informacji objętych załącznikiem nr 4 do niniejszego Zarządzenia,
4) sprawuje nadzór nad zgodnym z prawem przetwarzaniem danych osobowych w podległej komórce organizacyjnej Urzędu Gminy, zwłaszcza stosowania zasad szczególnej staranności przetwarzania danych określonych w art. 26 ustawy,
5) sprawuje nadzór nad realizowaniem procedur Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym w podległej komórce organizacyjnej.

**§ 7**

1.Osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do:
1) wykonywania czynności przetwarzania danych tylko w zakresie określonym w indywidualnym upoważnieniu do przetwarzania danych osobowych,
2) zapoznania się i stosowania Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym, co potwierdza złożeniem oświadczenia przechowywanego w aktach osobowych. Wzór oświadczenia stanowi załącznik nr 3do niniejszego Zarządzenia,
3) nieprzetwarzania danych osobowych w celach prywatnych.

2. Naruszenie obowiązków, o których mowa w ust. 1, w szczególności świadome udostępnienie danych osobowych osobie nieupoważnionej:
1) podlega sankcjom dyscyplinarnym,
2) sankcjom karnym, wynikającym zwłaszcza z art. 51-52 ustawy oraz art. 266 Kodeksu karnego,
3) uzasadnia rozwiązanie umowy o pracę bez wypowiedzenia.

**§ 8**

1. Przetwarzane danych osobowych ma miejsce wyłącznie w pomieszczeniach biurowych Urzędu Gminy z zastrzeżeniem ust.2.

2. Przetwarzanie danych osobowych poza obiektem Urzędu Gminy w komputerach przenośnych oraz na przenośnych nośnikach danych, nie jest dozwolone w miejscach nie zapewniających brak dostępu dla osób nieupoważnionych, a w szczególności w miejscach publicznych.

3. Zbiory danych osobowych, a także dokumenty, wydruki komputerowe oraz nośniki zawierające dane osobowe przechowywane są w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nieantywłamaniowymi), w meblach zamykanych na klucz.

4. Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się komputer główny, na którym dane osobowe przetwarzane są na bieżąco, w meblach zamykanych na klucz.

**§ 9**

1.Pomieszczenia biurowe w których przetwarzane są dane osobowe są:
1) przed rozpoczęciem pracy – sprawdzane, czy nie ma śladów włamania lub uszkodzenia. Takiemu samemu sprawdzeniu podlegają meble biurowe, w których przechowywane są dokumenty zawierające dane osobowe.
2) w trakcie godzin pracy - zamykane na czas nieobecności osoby zatrudnionej przy przetwarzaniu danych osobowych,
3) po zakończeniu pracy – sprawdzane, czy nie pozostały niezabezpieczone dokumenty, nośniki lub wydruki zawierające dane osobowe oraz zamknięcie szaf.
2. Osoby nieupoważnione przebywają w pomieszczeniach biurowych tylko w obecności osoby upoważnionej do przetwarzania danych osobowych lub Administratora Bezpieczeństwa Informacji.
3. Zasady postępowania z kluczami od pomieszczeń i mebli biurowych, o których mowa w § 9 określają odrębne przepisy.

4. Pomieszczenie serwerowni zabezpiecza się poprzez
1)wyposażenie w system alarmowy i klimatyzację,
2)zamontowanie zamka uniemożliwiającego niekontrolowany dostęp do pomieszczenia z zewnątrz.

**§ 10**

1. Wykonywanie wydruków komputerowych zawierających dane osobowe na drukarce systemowej lub stanowiskowej odbywa się pod kontrolą osoby je wykonującej.
2. Do przechowywania i rejestracji wydruków komputerowych należy stosować odpowiednio Instrukcję kancelaryjną z wyjątkiem wydruków wadliwych i próbnych, które należy zniszczyć w niszczarkach dokumentów

**§ 11**

1. W razie wystąpienia sytuacji losowych lub nieprzewidzianych oddziaływań czynników zewnętrznych na zasoby systemu, takich jak pożar, zalanie pomieszczeń, katastrofa budowlana, powódź osoba upoważniona do przetwarzania danych osobowych i odpowiedzialna za sprzęt komputerowy zobowiązana jest ten fakt zgłosić Administratorowi Bezpieczeństwa Informacji.
2. Administrator Bezpieczeństwa Informacji wskazuje:
a) sposób zabezpieczenia sprzętu komputerowego,
b) miejsce, w które należy przenieść zagrożony sprzęt komputerowy.
3. Po ustaniu sytuacji o których mowa w ust. 1 Administrator Bezpieczeństwa Informacji podejmuje działania mające na celu ponowne uruchomienie zabezpieczonego sprzętu komputerowego.

**§ 12**

1. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów je obsługujących oraz pomieszczeń, w których przetwarzane są dane osobowe stanowi załącznik nr 4 do niniejszego Zarządzenia.
2. Aktualizacja załącznika nr 4 nie wymaga zmiany Zarządzenia.

**§ 13**

1. Upoważnienia do przetwarzania danych w systemie informatycznym oraz hasła dostępu do systemu informatycznego, wydane są na podstawie stosownych postanowień Kierownika Urzędu Gminy
2. Kierownicy jednostek organizacyjnych Urzędu Gminy złożą w terminie do dnia 31.01.2012 r. do Sekretarza Gminy wnioski o wydanie upoważnienia do przetwarzania danych osobowych, o których mowa w § 6 ust. 4 pkt. 1 niniejszego Zarządzenia

**§ 14**

Wykonanie Zarządzenia powierzam kierownikom Urzędu Gminy Krzyżanowice, Administratorowi Bezpieczeństwa Informacji oraz Sekretarzowi, a nadzór nad wykonaniem Zarządzenia będę sprawował osobiście.

**§ 15**

Zarządzenie wchodzi w życie z dniem podpisania

# U Z A S A D N I E N I E

Obowiązek prowadzenia dokumentacji opisującej sposób przetwarzania danych osobowych określony został w art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. z 2002 r. Dz. U. Nr 101 poz. 926 z późn. zm.).

Sposób wykonania tego obowiązku został skonkretyzowany w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z 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. Nr 100, poz. 1024).

Funkcjonowanie wymienionych przepisów pozwoliło na określenie zarówno w doktrynie jak i w praktyce standardów, którym te dokumenty powinny odpowiadać.

Niniejsze Zarządzenie stanowi dostosowanie dotychczas funkcjonujących przepisów wewnętrznych w tym zakresie do obowiązujących wymagań.