Zarządzenie Nr 90/2010

Wójta Gminy Gniewino

z dnia 29 września 2010 r.

w sprawie ustalenia i wdrożenia polityki bezpieczeństwa informacji w Urzędzie Gminy Gniewino.

Na podstawie art. 31 oraz art. 33 ust. 3 w związku z art. 11a ust. 1 pkt 2 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2001 r. Nr 142, poz. 1591 ze zm.), art. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926) oraz § 4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024)

Wójt Gminy Gniewino

zarządza co następuje:

§ 1

Wprowadza się do użytku służbowego „Politykę Bezpieczeństwa Informacji w Urzędzie Gminy Gniewino" w brzmieniu stanowiącym załącznik do niniejszego zarządzenia.

§ 2

Zobowiązuje się wszystkich pracowników do przestrzegania Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Gniewino oraz postanowień ustawy o ochronie danych osobowych i przepisów wykonawczych wydanych na jej podstawie.

§ 3

Traci moc Zarządzenie Nr 4/99 Wójta Gminy Gniewino z dnia 1 października 1999r. w sprawie Instrukcji określającej sposób zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w formie elektronicznej oraz Instrukcji postępowania w sytuacji naruszenia zasad ochrony danych osobowych.

§ 4

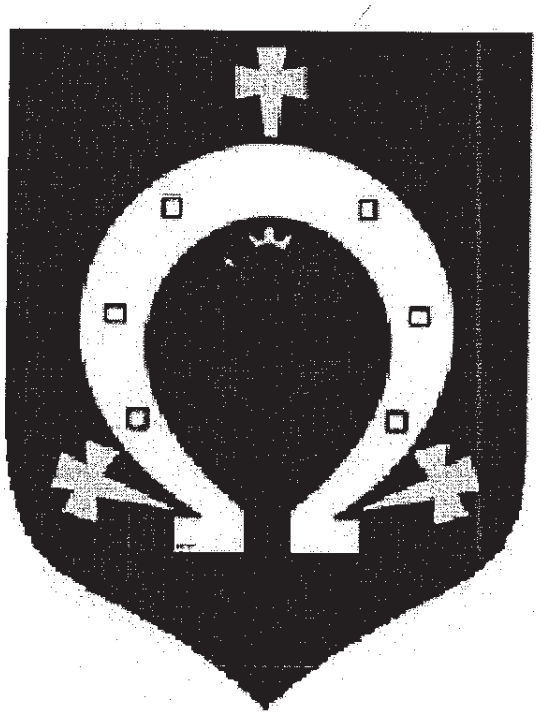
Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJT GMINY
mgr Zbigniew Walczak

KK

Załącznik do Zarządzenia Nr 90/2010 Wójta Gminy Gniewino
z dnia 29 września 2010r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI



URZĄD GMINY GNIEWINO

Załącznik do Zarządzenia Nr 90/2010 Wójta Gminy Gniewino
z dnia 29 września 2010r.

Wstęp

Polityka Bezpieczeństwa Informacji opracowana została na podstawie art. 36 ust.2 i art. 39a, ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, *(tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.),* oraz 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. z 2004 r. Nr 100, poz. 1024).*

Celem niniejszej Polityki Bezpieczeństwa jest określenie zasad przetwarzania danych osobowych jako zestaw praw, reguł, procedur i praktycznych doświadczeń regulujących sposób zarządzania danymi, ich ochrony i dystrybucji wewnątrz Urzędu Gminy Gniewino, jak i w kontaktach z otoczeniem. Polityka Bezpieczeństwa stanowi dokument odnoszący się całościowo do problemu zabezpieczenia danych osobowych u Administratora Danych.

Zawiera ona opis zastosowanych środków organizacyjnych i technicznych oraz mechanizmów ochrony danych osobowych przetwarzanych zarówno w zbiorach tradycyjnych (papierowych) jak i elektronicznych. Ponadto normuje procedury aktualizacji dokumentacji związanej z ochroną danych osobowych oraz wprowadza jednolite zasady wydawania upoważnień do przetwarzania danych osobowych oraz pozwala monitorować proces udostępniania informacji i inne aspekty związane z przetwarzaniem danych osobowych.

Stosowanie zasad zawartych w niniejszym dokumencie przez wszystkich użytkowników systemów informatycznych pozwala zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Definicje

Poniżej zestawiono najważniejsze pojęcia i definicje, które powinny być znane i stosowane w bieżącej pracy podczas przetwarzania danych osobowych przez wszystkich pracowników Urzędu Gminy Gniewino odpowiedzialnych za ochronę tych danych.

1) Ustawa – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.).
2) 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 (Dz. U. z 2004 r. Nr 100, poz. 1024).
3) Urząd — Urząd Gminy Gniewino.
4) Administrator Danych – Urząd, w którego imieniu zadania w zakresie ochrony danych osobowych wykonuje Wójt Gminy.
5) GIODO - Generalny Inspektor Ochrony Danych Osobowych.
6) Polityka Bezpieczeństwa Informacji – dokument opracowany na podstawie art. 39a ustawy, oraz § 3 pkt. 1 rozporządzenia.
7) Administrator Bezpieczeństwa Informacji (ABI) - osoba powołana zarządzeniem Wójta Gminy Gniewino, która odpowiada za bezpieczeństwo danych osobowych w systemie informatycznym Urzędu, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemów, w których przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.

8) Administrator Systemu Informatycznego (ASI) – osoba upoważniona przez ABI – administrator konkretnego systemu informatycznego przetwarzającego dane osobowe;
9) Dane osobowe – 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 albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.
10) Adekwatność danych – przetwarzanie danych osobowych niewychodzące poza zakres konieczny.
11) Celowość – oznacza, że dane osobowe mogą być przetwarzane tylko w tym celu, dla jakiego zostały zebrane.
12) Zabezpieczenie danych w systemie informatycznym – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
13) Integralność danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione, dodane lub usunięte w nieautoryzowany sposób.
14) Obszar przetwarzania danych osobowych – budynki, pomieszczenia lub części pomieszczeń Urzędu, w których są przetwarzane dane osobowe zarówno w formie papierowej, jak i elektronicznej.
15) Poufność danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.
16) Przetwarzanie danych osobowych – 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.
17) System - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych.
18) Bezpieczeństwo systemu - zapewnienie jego poufności, dostępności i integralności przy zastosowaniu środków technicznych i organizacyjnych.
19) Rozliczalność – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
20) Uwierzytelnienie – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
21) Usuwanie danych osobowych – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
22) Użytkownik systemu – pracownik Urzędu posiadający uprawnienia do przetwarzania danych osobowych w systemie informatycznym.
23) Zbiór danych osobowych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie.

Zasady ogólne

1) Administrator Danych jest odpowiedzialny za tworzenie, wdrażanie, administrację i interpretację Polityki Bezpieczeństwa Informacji.
2) Każdy użytkownik systemu zna przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz

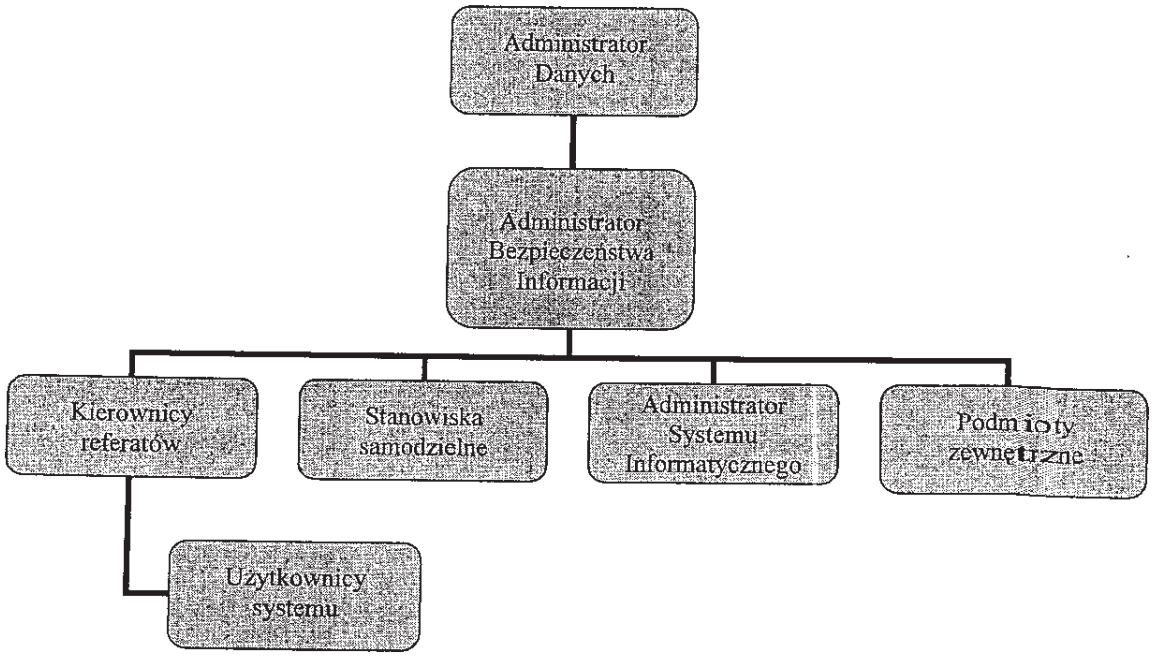
warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych oraz niniejszą Politykę Bezpieczeństwa Informacji.

3) Każdy użytkownik systemu spełnia kryteria dopuszczenia do informacji i podpisał stosowne oświadczenie o zachowaniu poufności.
4) Ochrona danych osobowych przetwarzanych w Urzędzie obowiązuje wszystkich użytkowników systemu, bez względu na zajmowane stanowisko oraz miejsce wykonywania jak również charakter stosunku pracy.
5) Użytkownicy systemu są zobligowani do stosowania niezbędnych środków zapobiegających ujawnieniu danych osobom nieupoważnionym.
6) Zachowanie tajemnicy obowiązuje zarówno podczas trwania stosunku pracy jak i po jego ustaniu.
7) Każdy użytkownik systemu posiada prawa dostępu do informacji ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań.
8) Każdy użytkownik systemu posiada wiedzę o systemie, do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych mu zadań.
9) Wszyscy użytkownicy systemu są świadomi konieczności ochrony zasobów informacyjnych Urzędu i aktywnie uczestniczą w tym procesie.
10) Za bezpieczeństwo poszczególnych elementów systemu odpowiadają konkretne osoby.
11) Prawo przebywania w określonych miejscach mają tylko osoby upoważnione.
12) System jest przygotowany na wszelkie zagrożenia. Niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających.
13) Skuteczne zabezpieczenie jest tylko wtedy, gdy stosuje się podejście kompleksowe, uwzględniające wszystkie stopnie i ogniwa ogólnie pojętego procesu przetwarzania informacji.
14) Polecenia Administratora Bezpieczeństwa Informacji muszą być bezwzględnie wykonywane przez wszystkich użytkowników systemu.

Załącznik do Zarządzenia Nr 90/2010 Wójta Gminy Gniewino
z dnia 29 września 2010r.

Struktura zarządzania bezpieczeństwem informacji

Poniższy schemat przedstawia organizację zarządzania bezpieczeństwem informacji w Urzędzie.



W powyższej strukturze możliwe jest wyróżnienie trzech poziomów działań:

1) Na poziomie **strategicznym** prowadzona jest generalna polityka bezpieczeństwa informacji, dlatego też w procesy decyzyjne tego poziomu zaangażowani są Administrator Danych i Administrator Bezpieczeństwa Informacji.
2) Na poziomie **taktycznym** tworzone są standardy bezpieczeństwa informacji i zasady kontroli ich wypełniania w stosowanych rozwiązaniach i systemach informatycznych. W te procesy decyzyjne zaangażowani są głównie kierownicy poszczególnych referatów.
3) Na poziomie **operacyjnym** prowadzona jest administracja bezpieczeństwem informacji pod kątem pełnego stosowania standardów bezpieczeństwa oraz rozwiązywania sytuacji zakłóceń wynikających z naruszenia tych standardów (intencjonalnego lub przypadkowego).

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

Przetwarzanie danych osobowych może odbywać się wyłącznie w obszarach do tego celu przeznaczonych. Poniższe zestawienie stanowi wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar w którym przetwarzane są dane osobowe oraz sposób zabezpieczeń poszczególnych budynków, pomieszczeń lub ich części.

Załącznik do Zarządzenia Nr 90/2010 Wójta Gminy Gniewino
z dnia 29 września 2010r.

Adres	Fizyczne środki ochrony	Nr pokoju	Fizyczne środki ochrony danych osobowych	Osoby odpowiedzialne za klucze
Urząd Gminy Gniewino, Gniewino, ul. Pomorska 8	1. Kraty w oknach na parterze 2. Kraty w drzwiach głównych i bocznych 3. Klucze do budynku i kod dostępu posiadają tylko upoważnione osoby 4. Wszystkie pomieszczenia biurowe zamykane na klucz 4. Alarm objęty monitoringiem sygnałów alarmowych	1		
		2	1.Szafa pancerna w której znajdują się wszystkie klucze do pomieszczeń Urzędu Gminy 2. Szafy drewniane na klucz 3. Kraty w oknach	Kunath Gabriela
		3	1. Szafy drewniane na klucz 2. Kraty w oknach 3. Klucze od pomieszczenia są przekazywane do sekretariatu	Kwaśniewska Mariola, Słowik Michał
		4	1. Szafy metalowe na klucz 2. Szafy drewniane na klucz 3. Kraty w oknach 4. Klucze od pomieszczenia przekazywane są codziennie do sekretariatu	Ewald Krystyna, Górkowska Irena, Napieraj Elżbieta
		5	1. Szafy drewniane na klucz 2. Kraty w oknach 3. Klucze od pomieszczenia przekazywane są codziennie do sekretariatu	Patelczyk Maria
		6	1. Szafy drewniane na klucz 3. Kraty w oknach 2. Klucze od pomieszczenia przekazywane są codziennie do sekretariatu	Marcinkiewicz Mirosław
		7	1. Szafy drewniane na klucz 3. Kraty w oknach 2. Klucze od pomieszczenia przekazywane są codziennie do sekretariatu	Weltrowska Genowefa
		8	1. Szafy drewniane na klucz 3. Kraty w oknach 2. Klucze od pomieszczenia przekazywane są codziennie do sekretariatu	Romanek Jacek

Załącznik do Zarządzenia Nr 90/2010 Wójta Gminy Gniewino
z dnia 29 września 2010r.

		9	1. Szafy metalowe na klucz 2. Szafy drewniane na klucz 3. Kraty w oknach 4. Klucze od pomieszczenia przekazywane są codziennie do sekretariatu	Mudlaff Elżbieta
		10	1. Szafy drewniane na klucz 2. Szafa pancerna 3. Kraty w oknach 4. Klucze od pomieszczenia przekazywane są codziennie do sekretariatu	Maksymiuk, Rutz Genowefa
		12	1. Szafy metalowe na klucz 2. Szafy drewniane na klucz 3. Klucze od pomieszczenia przekazywane są codziennie do sekretariatu	Wyszecka Gabriela
		14	1. Szafy drewniane na klucz 2. Klucze od pomieszczenia przekazywane są codziennie do sekretariatu	Płaczek Mirosława
		Archiwum	1. Akta osobowe znajdują się w pomieszczeniu zamykanym na klucz 2. Klucz znajduje się w pomieszczeniu nr 14	Płaczek Mirosława
		15	1. Szafy drewniane na klucz 2. Klucze od pomieszczenia przekazywane są codziennie do sekretariatu	Kochan Krzysztof
Urząd Gminy Gniewino, ul. Pomorska 20/4	1. Kraty w oknach 2. Kraty w drzwiach wewn. 3. Klucze posiadają tylko upoważnione osoby		1. Szafy drewniane na klucz 2. Kraty w oknach 3. Kraty w wewnętrznych drzwiach	Baranowska Grażyna, Gacek Danuta, Trocki Mirosław
Przychodnia Lekarska w Gniewinie, ul. Pomorska 40/1	1. Alarm	203	1. Szafy drewniane	Labudda Krystyna

Załącznik do Zarządzenia Nr 90/2010 Wójta Gminy Gniewino
z dnia 29 września 2010r.

Straż Gminna, Kostkowo, ul. Wejherowska 24A	1. Alarm	1	1. Kraty w oknach	
		2	1. Szafy metalowe na klucz 2. Szafa pancerna – sejf 3. Alarm	Borowiec Ilona

Zasady korzystania z komputerów przenośnych, na których są przetwarzane dane osobowe

W szczególnych przypadkach możliwe jest przetwarzanie danych osobowych poza wyznaczonym obszarem (np. na komputerach przenośnych) jednak wymaga to zgody indywidualnej Administratora Bezpieczeństwa Informacji. Zakres danych przetwarzanych na komputerze przenośnym oraz zakres uprawnień do przetwarzanych danych ustala przełożony użytkownika za wiedzą Administratora Bezpieczeństwa Informacji. Osoba korzystająca z komputera przenośnego w celu przetwarzania danych osobowych zobowiązana jest do zwrócenia szczególnej uwagi na zabezpieczenie przetwarzanych informacji, zwłaszcza przed dostępem do nich osób nieupoważnionych oraz przed zniszczeniem.

Użytkownik komputera przenośnego zobowiązany jest do:

1) transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia, a w szczególności:
   - transportowania komputera w bagażu podręcznym,
   - niepozostawiania komputera w samochodzie, przechowalni bagażu, itp,
   - zaleca się przenoszenie komputera w torbie przeznaczonej do przenoszenia komputerów przenośnych;
2) korzystania z komputera w sposób minimalizujący ryzyko podejrzenia przetwarzanych danych przez osoby nieupoważnione, w szczególności zabrania się korzystania z komputera w miejscach publicznych i w środkach transportu publicznego;
3) niezezwalania osobom nieupoważnionym do korzystania z komputera przenośnego, na którym przetwarzane są dane osobowe;
4) zabezpieczania komputera przenośnego hasłem;
5) blokowanie dostępu do komputera przenośnego w przypadku gdy nie jest on wykorzystywany przez pracownika;
6) kopiowania danych osobowych przetwarzanych na komputerze przenośnym do systemu informatycznego w celu umożliwienia wykonania kopii awaryjnej tych danych;
7) umożliwienia, poprzez podłączenie komputera do sieci informatycznej aktualizacji wzorców wirusów w programie antywirusowym;
8) utrzymania konfiguracji oprogramowania systemowego w sposób wymuszający korzystanie z haseł;
9) wykorzystywanie haseł odpowiedniej jakości zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym przetwarzającym dane osobowe;
10) zmianę haseł zgodnie z wymaganiami dla systemu informatycznego przetwarzającego dane osobowe.

Załącznik do Zarządzenia Nr 90/2010 Wójta Gminy Gniewino
z dnia 29 września 2010r.

Administrator bezpieczeństwa informacji zobowiązany jest do podjęcia działań mających na celu zabezpieczenie komputerów przenośnych, w szczególności aby:

1) dokonano konfiguracji oprogramowania na komputerach przenośnych w sposób wymuszający korzystanie z haseł, wykorzystywanie haseł odpowiedniej jakości zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym przetwarzającym dane osobowe oraz wymuszającym okresową zmianę haseł zgodnie z wymaganiami dla systemu informatycznego przetwarzającego dane osobowe;
2) dokonano instalacji i konfiguracji oprogramowania antywirusowego na komputerze przenośnym;
3) przeprowadzono aktualizację wzorców wirusów zgodnie z zasadami zarządzania programem antywirusowym.

Administrator bezpieczeństwa informacji jest odpowiedzialny za prowadzenie ewidencji komputerów przenośnych wykorzystywanych do przetwarzania danych osobowych. W szczególności ewidencja obejmuje:

1) typ i numer seryjny komputera przenośnego,
2) imię i nazwisko użytkownika komputera,
3) oprogramowanie zainstalowane na komputerze,
4) rodzaj i zakres danych osobowych przetwarzanych na komputerze przenośnym.

W razie zgubienia lub kradzieży pracownik zobowiązany jest do natychmiastowego powiadomienia administratora bezpieczeństwa informacji lub osoby uprawnionej zgodnie z zasadami informowania o naruszeniu ochrony danych osobowych.

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

Lp.	Nazwa zbioru	Prowadzący zbiór	Program zastosowany do przetwarzania danych osobowych
Urząd Gminy Gniewino, ul. Pomorska 20/4			
1	zamówienia publiczne, pisma urzędowe	Gacek Danuta	pakiet Office
2	ewidencja działalności gospodarczej, pisma urzędowe	Baranowska Grażyna	pakiet Office
3	azbest	Trocki Mirosław	Wojewódzka Baza Wyrobów i Odpadów zawierające azbest
	zestawienie odpadów		GOMiG
	umowy z firmami, pisma urzędowe		pakiet Office
Urząd Gminy Gniewino, Gniewino, ul. Pomorska 8			
4	ewidencja gruntów, budynków i lokali	Marcinkiewicz Mirosław	program geodezyjny EGBVWIN
	pisma urzędowe		pakiet Office
5	pisma urzędowe	Patelczyk Maria	pakiet Office
6	pisma urzędowe	Weltrowska Genowefa	pakiet Office
	ewidencja gruntów, budynków i lokali		program geodezyjny EGBVWIN

Załącznik do Zarządzenia Nr 90/2010 Wójta Gminy Gniewino
z dnia 29 września 2010r.

7	ewidencja gruntów, budynków i lokali	Romanek Jacek	program geodezyjny EGBVWIN
	pisma urzędowe		pakiet Office
8	ściągalność: wpłata prawna, rolna, nieruchomość	Górkowska Irena	GRAVIS
	pisma urzędowe		pakiet Office
9	wymiar podatku: nieruchomość, transport, rolny	Ewald Krystyna	GRAVIS
	ewidencja gruntów, budynków i lokali		program geodezyjny EGBVWIN
	pisma urzędowe		pakiet Office
10	płace, rozrachunki i finanse, środki trwałe	Napieraj Elżbieta	GRAVIS
	emisja ubezpieczeń społecznych, zdrowotnych i emerytalnych od płac pracowników		PŁATNIK
	miesięczne obowiązkowe wpłaty na państwowy fundusz ochrony osób niepełnosprawnych		PFRON
	faktury		przelewy, faktury
	czynsze mieszkaniowe		czynsze
	kontakt elektroniczny z bankiem		Home Banking
11	pisma urzędowe	Kwaśniewska Mariola	pakiet Office
12	pisma urzędowe	Słowik Michał	pakiet Office
13	pisma urzędowe	Orzeł Mikołaj	pakiet Office
14	pisma urzędowe	Kamiński Rafał	pakiet Office
15	sprawozdania, plany budżetowe	Maksymiuk Marianna	BUDŻET
	księgowanie		GRAVIS
	przesyłanie zbiorczych informacji do RIO		BESTI@
	pisma urzędowe		pakiet Office
16	sprawozdania, plany budżetowe	Rutz Genowefa	BUDŻET
	księgowanie		GRAVIS
	przesyłanie zbiorczych informacji do RIO		BESTI@
	pisma urzędowe		pakiet Office

17	ewidencja ludności	Mudlaff Elżbieta	ELUD
	rejestr wyborców		WYB.
	dowody osobiste		SWDO
	pisma urzędowe		pakiet Office
18	kadry, pisma urzędowe	Płaczek Mirosława	pakiet Office
19	pisma urzędowe	Kochan Krzysztof	pakiet Office
Przychodnia Lekarska w Gniewinie, ul. Pomorska 40/1			
20	dodatki mieszkaniowe	Labuda Krystyna	RADIX
	stypendia, pisma urzędowe		pakiet Office
Straż Gminna, Kostkowo, ul. Wejherowska 24A			
21	pisma urzędowe	Ławinska Małgorzata, Borowiec Ilona	pakiet Office

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

Opis struktury zbiorów danych zawarty jest w załącznikach do niniejszego dokumentu:
Nr 1 – program Płatnik,
Nr 2 – program Besti@
Nr 3 – program GOMIG Odpady
Nr 4 – program EGBVWIN Geodezja
Nr 5 – programy GRAVIS

Sposób przepływu danych pomiędzy poszczególnymi systemami

1) Stacje robocze w Urzędzie połączone są w sieć logiczną za pośrednictwem sieci Ethernet.
2) W budynkach Urzędu występuje tylko jedna sieć lokalna z dostępem tylko dla pracowników Urzędu, posiada dopuszczenie do serwerów, na których położone są bazy zawierające dane osobowe.
3) W systemie informatycznym Urzędu występują dwa serwery pełniące role bazodanowych. Serwery znajdują się w pomieszczeniu Serwerowni w budynku przy ul. Pomorskiej 8. Stacje robocze w budynku przy ul. Pomorskiej 8 są przyłączone do Serwerowni za pomocą dedykowanego, wydzielonego i całkowicie izolowanego łącza światłowodowego. Scentralizowanie położenia serwerów baz danych pozwala na lepszą kontrolę nad tworzeniem kopii zapasowych.
4) Możliwe przepływy danych między oprogramowaniem przetwarzającym bazy danych zawierające dane osobowe:
   - system DocFlow (eUrząd) <-> uprawnione stacje robocze (wydzielona baza danych do obsługi elektronicznego obiegu dokumentów);
   - programy systemu GRAVIS (podatki, księgowość) <-> wyłącznie stacje robocze referatu FK;
   - program Home Banking <-> uprawnione stacje robocze referatu FK – wymiana danych operacyjnych z systemem bankowości elektronicznej Kaszubskiego Banku Spółdzielczego w Wejherowie za pośrednictwem dedykowanego łącza modemowego realizowanego z wytypowanych, uprawnionych stacji roboczych, zabezpieczone bankową procedurą łączenia i szyfrowania danych;

- program „Płatnik" realizujący zadania ewidencji danych oraz wymiany danych z systemem ZUS za pośrednictwem łącza internetowego w oparciu o technologię bezpośredniej wymiany danych zabezpieczonej szyfrowaniem przesyłu za pomocą kwalifikowanego podpisu elektronicznego, jest zainstalowany na jednej stacji roboczej w referacie FK;
- wymiana danych (export-import) pomiędzy oprogramowaniem systemu GRAVIS „Płace" i programem ZUS „Płatnik" odbywa się wewnętrznie na jednym stanowisku roboczym w referacie FK, na którym zainstalowane są obie bazy danych. Nie występuje tu transfer danych poza obszar tego stanowiska roboczego.

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

Wszystkie programy wykorzystywane do przetwarzania danych osobowych posiadają własny system identyfikacji użytkowników. Każdy użytkownik przetwarzający dane osobowe posiada swój własny identyfikator utworzony w programie, w którym przetwarza dane. Identyfikator taki zabezpiecza dane przed niepowołanym dostępem.
Poszczególne systemy za pomocą mechanizmu rejestracji zapamiętują informacje związane z czasem pracy użytkowników. Pracownicy UG Gniewino mają przydzielone zakresy obowiązków, zgodnie z którymi odpowiadają za przetwarzanie określonych baz danych osobowych. W każdym przypadku jest wyznaczona jedna osoba (oraz osoby zastępujące ją na czas nieobecności) odpowiedzialna za konkretny zbiór danych, posiadająca niepowtarzalny identyfikator, który umożliwia rozliczalność wprowadzanych zmian.

Zasady ogólne:

1) Przetwarzać dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych.
2) Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
3) Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje lub posługiwał.
4) Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.

Środki organizacyjne:

1) Wprowadzenie instrukcji dla pracowników zatrudnionych przy przetwarzaniu danych osobowych.
2) Powołanie Administratora Bezpieczeństwa Informacji i Administratora Systemu Informatycznego odpowiedzialnych za działania organizacyjne i środki techniczne zapewniające odpowiedni poziom bezpieczeństwa danych osobowych.
3) Prowadzenie ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych.
4) Kontrola dostępu do pomieszczeń, w których przetwarzane są dane osobowe oraz ścisła kontrola dostępu do pomieszczeń, w których znajdują się serwery.
5) Zgodne z „Instrukcją zarządzania systemem" tworzenie kopii archiwalnych baz danych zawierających dane osobowe.

6) Bardzo dokładne testowanie modyfikacji oprogramowania przed wdrożeniem go do użytku operacyjnego zarówno pod kątem poprawności działania jak i podatności na „ataki" z zewnątrz.

Sposób postępowania w zakresie komunikacji w sieci komputerowej:

Dane osobowe są przesyłane w sieci informatycznej dedykowanej do obsługi systemu informatycznego przetwarzającego te dane (intranet). Sieć ta jest odseparowana od pozostałej infrastruktury teleinformatycznej poprzez fizyczne rozdzielenie infrastruktury ethernetowej.
Ruch dla usług publicznych (strefa DMZ) jest chroniony przy pomocy access-list na routerze, bez udostępniania serwerów znajdujących się w sieci.
Ponadto cały ruch do sieci dedykowanej przechodzi przez urządzenie pełniące rolę zapory ogniowej (firewall), gdzie jest filtrowany i translowany na lokalną klasę adresów. Dodatkowo serwery sieci lokalnej chronione przez własne zapory ogniowe (firewall) uniemożliwiające nieautoryzowany dostęp do danych znajdujących się na tych serwerach.
Stacje robocze w dedykowanej sieci do obsługi danych osobowych znajdują się wewnątrz sieci intranetowej niedostępnej z internetu.
Przy przesyłaniu danych osobowych poza siecią dedykowaną do transferu danych osobowych wymagane jest zastosowanie szczególnych wymagań w zakresie bezpieczeństwa. Obejmują one:

- zatwierdzenia w formie pisemnej lub w formie elektronicznej przez upoważnionego użytkownika systemu celu wysłania danych osobowych,
- zastosowanie mechanizmów szyfrowania danych osobowych.

W przypadku stosowania mechanizmów kryptograficznych administrator bezpieczeństwa informacji określa wymagania w zakresie materiału kryptograficznego stosowanego do ochrony danych osobowych. Jeżeli nie określi on innych wymagań stosuje się:

- przy szyfrowaniu symetrycznym algorytm AES z kluczem 256 bitów,
- przy szyfrowaniu asymetrycznym algorytm RSA z kluczem 1024 bity,
- funkcję skrótu SHA-1.

W wypadku gdy podmiot zewnętrzny, z którym wymieniane są dane osobowe korzysta z innych mechanizmów kryptograficznych niż stosowane w OPI, możliwe jest zastosowanie tych mechanizmów lub mechanizmów z nimi zgodnych pod warunkiem zapewnienia zbliżonej do obowiązującej ochrony przesyłanych danych osobowych. W tym celu administrator systemu informatycznego lub osoba specjalnie do tego celu wyznaczona, może przeprowadzić analizę poziomu bezpieczeństwa mechanizmu kryptograficznego oraz zgodności tego mechanizmu z komponentami systemu informatycznego.
W przypadku wystąpienia uzasadnionego podejrzenia przechwycenia kluczy kryptograficznych lub dostania się ich w niepowołane ręce pracownik zobowiązany jest poinformować o tym fakcie Administratora Bezpieczeństwa Informacji lub osoby przez niego uprawnione zgodnie z wytycznymi opisanymi w rozdziale „Zasady postępowania w przypadku naruszenia ochrony danych osobowych".

Zasady postępowania w przypadku naruszenia ochrony danych osobowych

Każdy pracownik biorący udział w przetwarzaniu danych osobowych w systemie informatycznym jest odpowiedzialny za bezpieczeństwo tych danych. W szczególności osoba, która zauważyła zdarzenie mogące być przyczyną naruszenia ochrony danych osobowych lub mogące spowodować naruszenie bezpieczeństwa danych, zobowiązana jest do natychmiastowego poinformowania Administratora Bezpieczeństwa Informacji lub Administratora Systemu Informatycznego.

Załącznik do Zarządzenia Nr 90/2010 Wójta Gminy Gniewino
z dnia 29 września 2010r.

O naruszeniu ochrony danych osobowych mogą świadczyć następujące symptomy:

- brak możliwości uruchomienia przez użytkownika aplikacji pozwalającej na dostęp do danych osobowych,
- brak możliwości zalogowania się do tej aplikacji,
- ograniczone, w stosunku do normalnej sytuacji, uprawnienia użytkownika w aplikacji (na przykład brak możliwości wykonania pewnych operacji normalnie dostępnych użytkownikowi) lub uprawnienia poszerzone w stosunku do normalnej sytuacji,
- wygląd aplikacji inny niż normalnie,
- inny zakres danych niż normalnie dostępny dla użytkownika – dużo więcej lub dużo mniej danych,
- znaczne spowolnienie działania systemu informatycznego,
- pojawienie się niestandardowych komunikatów generowanych przez system informatyczny,
- ślady włamania lub prób włamania do obszaru, w którym przetwarzane są dane osobowe,
- ślady włamania lub prób włamania do pomieszczeń, w których odbywa się przetwarzanie danych osobowych, w szczególności do serwerowni oraz do pomieszczeń, w których przechowywane są nośniki kopii zapasowych,
- włamanie lub próby włamania do szafek, w których przechowywane są – w postaci elektronicznej lub papierowej – nośniki danych osobowych,
- zagubienie bądź kradzież nośnika danych osobowych,
- zagubienie bądź kradzież nośnika materiału kryptograficznego (karty mikroprocesorowej, dyskietki itp.),
- kradzież sprzętu informatycznego, w którym przechowywane są dane osobowe,
- informacja z systemu antywirusowego o zainfekowaniu systemu informatycznego wirusami,
- fizyczne zniszczenie lub podejrzenie zniszczenia elementów systemu informatycznego przetwarzającego dane osobowe na skutek przypadkowych lub celowych działań albo zaistnienia działania siły wyższej,
- podejrzenie nieautoryzowanej modyfikacji danych osobowych przetwarzanych w systemie informatycznym.

W wypadku wystąpienia powyższych symptomów, jak również innych objawów, które zdaniem pracownika mogą wskazywać na zagrożenie bezpieczeństwa danych osobowych, należy natychmiast powiadomić Administratora Bezpieczeństwa Informacji lub Administratora Systemu Informatycznego.

Informacja o pojawieniu się zagrożenia jest przekazywana przez pracownika osobiście, telefonicznie lub pocztą elektroniczną. Taka informacja powinna zawierać imię i nazwisko osoby zgłaszającej oraz zauważone symptomy zagrożenia. W przypadku, gdy zgłoszenie o podejrzeniu incydentu otrzyma osoba inna niż Administrator Bezpieczeństwa Informacji, jest ona zobowiązana poinformować o tym fakcie Administratora Bezpieczeństwa Informacji.

Po otrzymaniu zgłoszenia o wystąpieniu symptomów wskazujących na możliwość zaistnienia w OPI naruszenia bezpieczeństwa danych osobowych Administrator Bezpieczeństwa Informacji we współpracy z Administratorem Systemu Informatycznego, jest zobowiązany do podjęcia kroków w celu:

- wyjaśnienia zdarzenia, a w szczególności czy miało miejsce naruszenie ochrony danych osobowych,
- wyjaśnienia przyczyn naruszenia bezpieczeństwa danych osobowych i zebranie ewentualnych dowodów, a w szczególności, gdy zdarzenie było związane z celowym działaniem pracownika bądź osób trzecich,

- zabezpieczenia systemu informatycznego przed dalszym rozprzestrzenianiem się zagrożenia,
- usunięcia skutków incydentu i przywróceniu pierwotnego stanu systemu informatycznego (to jest stanu sprzed incydentu).

Administrator Bezpieczeństwa Informacji we współpracy z Administratorem Systemu Informatycznego podejmuje działania zmierzające do wyjaśnienia zgłoszonego zdarzenia:

- przeprowadzenia analizy poprawności funkcjonowania systemu informatycznego,
- przeprowadzenie analizy danych osobowych przetwarzanych w systemie informatycznym,
- zabezpieczenie danych przetwarzanych w systemie informatycznym, w szczególności danych konfiguracyjnych tego systemu.

Administrator Bezpieczeństwa Informacji określa na podstawie zebranych informacji przyczyny zaistnienia incydentu. Jeżeli incydent był spowodowany celowym działaniem, jest on zobowiązany do pisemnego powiadomienia Administratora Danych Osobowych w OPI, który może poinformować organy uprawnione do ścigania przestępstw o fakcie celowego naruszenia bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym.
System informatyczny, którego prawidłowe działanie zostało odtworzone powinien zostać poddany szczegółowej obserwacji w celu stwierdzenia całkowitego usunięcia symptomów incydentu. Administrator Bezpieczeństwa Informacji prowadzi ewidencję interwencji związanej z zaistniałymi incydentami w zakresie bezpieczeństwa danych osobowych. Ewidencja taka obejmuje następujące informacje:

- imię i nazwisko osoby zgłaszającej incydent,
- imię i nazwisko osoby przyjmującej zgłoszenie incydentu,
- datę zgłoszenia incydentu,
- przeprowadzone działania wyjaśniające przyczyny zaistnienia incydentu,
- wyniki przeprowadzonych działań,
- podjęte akcje naprawcze i ich skuteczność.

Administrator Bezpieczeństwa Informacji odpowiedzialny jest za przeprowadzenie przynajmniej raz w roku analizy zaistniałych incydentów w celu:

- określenia skuteczności podejmowanych działań wyjaśniających i naprawczych,
- określenie wymaganych działań zwiększających bezpieczeństwo systemu informatycznego i minimalizujących ryzyko zaistnienia incydentów,
- określenie potrzeb w zakresie szkoleń administratorów systemu i użytkowników systemu informatycznego przetwarzającego dane osobowe.