Zarządzenie Nr 42/2008
Burmistrza Gminy i Miasta Susz
z dnia 6 maja 2008 rok

w sprawie: wprowadzenia do użytku służbowego instrukcji dotyczących ochrony danych osobowych w Urzędzie Gminy i Miasta Susz.

Na podstawie art. 31 oraz art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2002 r. Nr 142, poz. 1591 ze zm.) i § 4 oraz § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. Nr 100, poz. 1024) - zarządza się co następuje:

§ 1.

1. Wprowadza się do użytku służbowego „Politykę bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy i Miasta Susz" w brzmieniu stanowiącym załącznik nr 1 do zarządzenia.
2. Wprowadza się do użytku służbowego „Instrukcję określającą sposób zarządzania systemami informatycznymi, służącymi do przetwarzania danych w Urzędzie Gminy i Miasta Susz" w brzmieniu stanowiącym załącznik nr 2 do zarządzenia.
3. Wprowadza się do użytku służbowego „Instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Gminy i Miasta Susz" w brzmieniu stanowiącym załącznik nr 3 do zarządzenia.

§ 2.

Zobowiązuje się pracowników przetwarzających dane osobowe do przestrzegania przepisów określonych w dokumentach, o których mowa w § 1.

§ 3.

Zobowiązuje się Kierowników Referatów Urzędu Gminy i Miasta Susz, w których przetwarzane są dane osobowe do sprawowania nadzoru nad ich ochroną oraz do współpracy z Administratorem Bezpieczeństwa Informacji w tym zakresie.

§ 4.

Wykonanie zarządzenia powierza się Sekretarzowi Gminy i Miasta Susz.

§ 5.

Zarządzenie wchodzi w życie z dniem podjęcia.

Burmistrz Gminy i Miasta
/-/ Jan Sadowski

Załącznik nr 1 do zarządzenia nr 42/2008
Burmistrza GiM Susz z dnia 6 maja 2008 r.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH PRZETWARZANYCH W SYSTEMIE INFORMATYCZNYM

URZĄD GMINY i MIASTA SUSZ

SPIS TREŚCI

Rozdział I
Postanowienia ogólne

1. **Określenia i skróty użyte w Polityce bezpieczeństwa oznaczają:**
   1) **Administrator Danych Osobowych** – Burmistrz Gminy i Miasta Susz, zwany dalej Administratorem.
   2) **Administrator Bezpieczeństwa Informacji, zwany dalej ABI** – osoba wyznaczona przez Administratora lub osobę upoważnioną, odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych Urzędu Gminy i Miasta w Suszu, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemów oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w tych systemach oraz odpowiedzialna za sprawność, konserwacje i wdrażanie technicznych zabezpieczeń systemów informatycznych, w których przetwarzane są dane osobowe w zbiorach komórek organizacyjnych Urzędu Gminy i Miasta w Suszu.
   3) **Osoba upoważniona lub użytkownik systemu, zwany dalej użytkownikiem** – osoba posiadająca upoważnienie wydane przez Administratora lub osobę upoważnioną przez niego i dopuszczona w zakresie w nim wskazanym, jako użytkownik do przetwarzania danych osobowych w systemie informatycznym komórki organizacyjnej Urzędu Gminy i Miasta w Suszu.
   4) **Przełożony użytkownika, zwany dalej przełożonym** – kierownik komórki organizacyjnej Urzędu Gminy i Miasta Susz lub bezpośredni przełożony.
   5) **System informatyczny, zwany dalej systemem -** zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
   6) **Zabezpieczenie systemu informatycznego** – wdrożenie przez Administratora stosownych środków organizacyjnych i technicznych w celu zabezpieczenia zasobów oraz ochrony danych przed dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem przez osobę trzecią.
   7) **Przetwarzanie danych osobowych** – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, udostępnianie i usuwanie, a zwłaszcza tych, które są wykonywane w systemach informatycznych.
2. Celem niniejszej polityki jest określenie podstawowych zasad bezpiecznego przetwarzania danych osobowych w systemie informatycznym Urzędu Gminy o Miasta w Suszu. Wszelkie dokumenty określające zasady przetwarzania danych osobowych w systemie informatycznym winny być zgodne z niniejszą polityką.
3. Polityka ta została opracowana i wdrożona ze względu na fakt, iż Burmistrz GiM jest administratorem danych osobowych, w rozumieniu ustawy z dnia 29 sierpnia 1997r., o ochronie danych osobowych. Niniejsza polityka dotyczy wszystkich osób biorących udział w sposób bezpośredni lub pośredni w przetwarzaniu danych osobowych w systemie informatycznym w Urzędzie.
4. Polityka ta oraz związane z nią dokumenty zostały opracowane zgodnie z wymaganiami obowiązujących przepisów prawnych, w szczególności zaś:
   1) Ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych ,zwanej dalej Ustawą,
   2) Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r, w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i

organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych

5. Burmistrz Gminy i Miasta Susz wyznacza Administratora Bezpieczeństwa Informatycznego (ABI) w celu sprawowania nadzoru nad przestrzeganiem obowiązujących zasad bezpieczeństwa danych osobowych, koordynacji procesów związanych z zarządzaniem systemem informatycznym przetwarzającym dane osobowe.

6. Wszystkie osoby biorące bezpośredni lub pośredni udział w procesie przetwarzania danych osobowych w systemie informatycznym są odpowiedzialne za właściwe zabezpieczenie tych danych.

7. Zabezpieczenie danych osobowych w systemie informatycznym obejmuje:

1) ochronę poufności rozumianej jako zabezpieczenie informacji przed dostępem do niej osób nieuprawnionych,

2) ochronę integralności rozumianej jako zabezpieczenie informacji przed wprowadzeniem przypadkowych lub celowych zmian powodujących jej zafałszowanie,

3) ochronę dostępności rozumianej jako zabezpieczenie informacji przed jej zniszczeniem, jak również zapewnienie takiego działania systemu informatycznego, aby dane osobowe były dostępne dla osób upoważnionych do dostępu do nich, a także do ich przetwarzania.

8. Przetwarzanie danych osobowych w systemach informatycznych jest dopuszczalne pod warunkiem:

1) spełnienia szczegółowych zaleceń dotyczących systemów informatycznych, posiadania przez te systemy mechanizmów pozwalających na realizację procesów zabezpieczenia danych osobowych opisanych w niniejszej polityce, jak również w dokumentach z nią związanych,

2) przetwarzania danych osobowych w zakresie dopuszczalnym ze względu na zapisy Ustawy.

9. Systemy informatyczne przetwarzające dane osobowe umieszczone są w wydzielonych strefach. Pracownicy upoważnieni do dostępu do stref zobowiązani są do niewpuszczania na teren strefy osób nieposiadających zgody Administratora danych osobowych lub ABI.

10. Dostęp użytkowników do systemu informatycznego przetwarzającego dane osobowe jest kontrolowany za pomocą mechanizmów uwierzytelniania, autoryzacji i rozliczalności. Podstawą uwierzytelniania użytkownika jest wykorzystanie unikalnego dla użytkownika identyfikatora i hasła. Hasło nie może być przekazane przez użytkownika jakiejkolwiek innej osobie, jedynym wyjątkiem jest przekazywanie przez Administratora tymczasowego hasła użytkownikowi. Autoryzacja użytkownika odbywa się na podstawie nadanych przez ABI przywilejów użytkownika. System informatyczny przetwarzający dane osobowe jest wyposażony w mechanizmy pozwalające jednoznacznie przypisać wykonanie określonych operacji na danych osobowych konkretnemu użytkownikowi.

11. Wszelkiego rodzaju nośniki danych osobowych, które są przekazywane osobom lub podmiotom nieupoważnionym do otrzymania tych danych, lub też gdy istnieje podejrzenie, że mogą się one znaleźć w rękach osób nieupoważnionych (na przykład w procesie likwidacji), pozbawia się danych lub doprowadza się do stanu uniemożliwiającego ich odczytanie. Za pozbawienie zapisu odpowiada osoba przekazująca nośnik lub odpowiadająca za realizację działań, w których wyniku nośnik może stać się dostępny dla osób nieupoważnionych. W razie gdy przekazanie nośnika jest związane z jego naprawą lub konserwacją albo naprawą i konserwacją urządzenia, którego częścią składową jest nośnik, dopuszczalne jest pozostawienie zapisanych danych pod warunkiem sprawowania nadzoru przez ABI lub upoważnionego przez Administratora pracownika podczas przeprowadzania naprawy lub konserwacji.

12. Dane osobowe zabezpieczane są przez tworzenie kopii awaryjnych.Za poprawność przebiegu procesu tworzenia kopii, jak również za zabezpieczenie składowanych nośników kopii i ich udostępnianie odpowiada ABI.

13. Wszelkiego rodzaju nośniki danych osobowych, w tym również kopie zapasowe danych osobowych muszą być przechowywane w sposób zapewniający odpowiednią ochronę przed dostępem osób niepowołanych oraz przed celowym lub przypadkowym zniszczeniem.

14. W wypadku wystąpienia przypadkowego lub celowego naruszenia bezpieczeństwa danych osobowych administrator bezpieczeństwa informacji jest odpowiedzialny za przeprowadzenie procesu usuwania skutków naruszenia bezpieczeństwa z uwzględnieniem wykrycia przyczyn zaistniałego incydentu, przekazania Administratorowi informacji o ewentualnych sprawcach oraz przeanalizowania możliwości wprowadzenia zabezpieczeń redukujących ryzyko wystąpienia w przyszłości podobnego incydentu. Każda osoba, która zauważy naruszenia bezpieczeństwa danych osobowych, a w szczególności:

1) ujawnienie lub możliwość ujawnienia danych osobowych osobom nieupoważnionym

2) zafałszowanie danych osobowych lub możliwość ich zafałszowania

3) zniszczenia lub możliwość zniszczenia danych osobowych

4) zablokowania lub możliwość zablokowania pracy systemu informatycznego zobowiązana jest natychmiast powiadomić ABI lub osoby przez niego upoważnione.

5) w szczególności naruszenie bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym obejmuje wprowadzenie do systemu wirusów lub innych wrogich kodów, jak również dostęp do systemu osób niepowołanych (fizyczny – przez bezpośredni dostęp do komputera, na którym przetwarzane są dane osobowe, oraz logiczny – poprzez dostęp do danych za pośrednictwem sieci informatycznych).

Szczegółowe zasady reagowania na incydenty związane z naruszeniem zasad bezpieczeństwa regulowane są w „Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych".

15. ABI jest odpowiedzialny za prowadzenie działań zmierzających do zabezpieczenia systemu informatycznego przetwarzającego dane osobowe przed zainfekowaniem wirusami lub innymi niebezpiecznymi kodami, a także ma prawo ograniczać uprawnienia użytkowników, w szczególności w zakresie wymiany informacji z wykorzystaniem publicznych sieci informatycznych, jeżeli może to wpłynąć na redukcję ryzyka wprowadzenia wirusów lub innych wrogich kodów.

16. Pracownicy Urzędu Gminy i Miasta w Suszu korzystający z systemu informatycznego są zobowiązani do stosowania się do szczegółowych zaleceń w zakresie ochrony antywirusowej, a także do przedmiotowych zaleceń wydawanych przez ABI.

Rozdział II
Obszar przetwarzania danych osobowych

1. Obszar przetwarzania danych osobowych w Urzędzie Gminy i Miasta w Suszu stanowią biura budynku przy ul. Wybickiego 6 :

- Parter - pokoje nr: 2, 4,
- I Piętro - pokoje nr: 103, 104, 106, 107, 108, 110, 111A, 111D
- II Piętro - pokoje nr: 203, 208, 209, 210, 212

Rozdział III
Wykaz zbiorów danych osobowych

1. **Referat Spraw Obywatelskich:**
   W Referacie Spraw Obywatelskich przetwarzane są dane osobowe zgodnie z ustawą o Ewidencji Ludności (Dz. U z 2001, nr 87, poz. 960), w postaci papierowej – Karta Osobowa Mieszkańca oraz w postaci elektronicznej – program PUMA-moduł Ewidencja Ludności – pracujący w architekturze klient (systemy Windows) – serwer (SUSE Linux Enterprise Server).

2. **Referat Organizacyjny:**
   W Referacie Organizacyjnym przetwarzane są dane osobowe pracowników Urzędu Gminy i Miasta w Suszu, zgodnie z ustawą z dnia 26 czerwca 1974 r. – kodeks pracy (Dz. U. nr 24, poz. 141 z późn. zm.), w postaci papierowej – akta pracownika oraz w postaci elektronicznej – program KADRY (pracujący pod kontrolą systemu sieciowego NetWare SBS 6.0), dane w archiwum w postaci papierowej.

3. **Referat Finansowy i Budżetu:**
   W Referacie Finansowym i Budżetu przetwarzane są dane osobowe płatników opłat i podatków, zgodnie z Rozporządzeniem Ministra Finansów z dnia 22 kwietnia 2004 r. w sprawie ewidencji podatkowej nieruchomości (Dz. U. z 2004 r. Nr 107, poz. 1138) oraz zgodnie z ustawą z dnia 26 czerwca 1974 r. – kodeks pracy (Dz. U. nr 24, poz. 141 z późn. zm.) w postaci papierowej – wydruki komputerowe oraz elektronicznie. Do przetwarzania danych osobowych służy oprogramowanie: „PODATKI", „KASA", „KADRY", „KADRY i PŁACE – OŚWIATA", „CZYNSZE", „HOME BANKING", „PŁATNIK" , „F-K" (pracujące pod kontrolą systemu sieciowego NetWare SBS 6.0).

4. **Urząd Stanu Cywilnego:**
   W Urzędzie Stanu Cywilnego przetwarzane są dane osobowe zgodnie z prawem o aktach stanu cywilnego (Dz. U. z 2004 r. Nr 161, poz. 1688), w postaci papierowej – Księga Stanu Cywilnego oraz w postaci elektronicznej – program „PB-USC", (pracujący pod kontrolą systemu Windows – baza danych MySQL na serwerze SUSE Linux Enterprise Server, Ewidencja działalności gospodarczej (pracujący pod kontrolą systemu Windows – aplikacja i baza danych).

5. **Referat Nieruchomości i Rolnictwa**
   W Referacie Nieruchomości i Rolnictwa przetwarzane są dane osobowe w postaci elektronicznej – program „GEO", (pracujący pod kontrolą systemu sieciowego NetWare SBS 6.0).
6. **Referat Promocji i Spraw Społecznych**
   W Referacie Promocji i Spraw Społecznych przetwarzane są dane osobowe w postaci elektronicznej – program „Świadczenia rodzinne moduł stypendia", (pracujący pod kontrolą systemu Windows – aplikacja i baza danych).

Rozdział IV
Opis struktury zbiorów

Opis struktur zbiorów danych osobowych stanowi załącznik do niniejszego dokumentu.

Rozdział V

Sposób przepływu danych pomiędzy poszczególnymi systemami służącymi do przetwarzania danych osobowych

1. Dane do systemu Ewidencja Ludności (moduł systemu PUMA) są wprowadzane z formularzy (wniosków) wypełnianych przez petentów. Moduł ten dostarcza danych osobowych pozostałym modułom systemu PUMA.

2. Dane z systemu „KADRY", „KADRY i PŁACE – OŚWIATA" zasilają systemy „Płatnik", „Home Banking". Dane są wprowadzane na zasadzie export-import, z wydruków komputerowych oraz formularzy i wniosków wypełnianych przez pracowników.

3. Dane do programów PODATKI i CZYNSZE są wprowadzane z odpowiednich deklaracji i wniosków. Dane z tych systemów przekazywane są do systemu KASA w celu realizacji płatności.

Rozdział VI

Środki techniczne i organizacyjne niezbędne do zapewnienia poufności i rozliczania danych

1. **Środki ochrony fizycznej:**
   1) budynek, poza godzinami pracy, jest zamykany i jest pod kontrolą systemu alarmowego;
   2) urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych zamkami;
2. **Środki sprzętowe i informatyczne:**
   1) zastosowano niszczarki dokumentów;
   2) zastosowano sieć lokalną typu gwiazda;
   3) dane są przetwarzane w sposób scentralizowany;
3. **Środki ochrony w ramach oprogramowania systemu:**
   1) dostęp fizyczny do baz danych osobowych zastrzeżony jest wyłącznie dla ABI;
   2) konfiguracja systemu umożliwia użytkownikom dostęp do danych osobowych tylko za pośrednictwem aplikacji;
   3) system operacyjny serwera pozwala zdefiniować prawa dostępu do zasobów systemu;
   4) zastosowano działający w „tle" program antywirusowy na komputerach użytkowników;
4. **Środki ochrony w ramach narzędzi baz danych:**
   1) automatycznie rejestrowany jest identyfikator użytkownika wprowadzającego dane;
   2) dla każdego użytkownika jest ustalony odrębny identyfikator i hasło;
   3) zdefiniowano użytkowników oraz ich prawa dostępu do danych osobowych;

5. Środki organizacyjne:

1) wyznaczono administratora bezpieczeństwa informacji ABI ;
2) osoby upoważnione do przetwarzania danych osobowych są przed dopuszczeniem ich do tych danych szkolone w zakresie obowiązujących przepisów o ochronie danych osobowych oraz procedur przetwarzania danych;
3) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych;
4) ustalono instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
5) zdefiniowano procedury postępowania w sytuacji naruszenia ochrony danych osobowych.

Załącznik nr 2 do zarządzenia nr 42/2008
Burmistrza GiM Susz z dnia 6 maja 2008 r.

INSTRUKCJA
określająca sposób zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych w Urzędzie Gminy i Miasta Susz.

Spis treści:

Rozdział 1
Postanowienia ogólne

§ 1.

Niniejsza „Instrukcja zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych w Urzędzie Gminy i Miasta Susz", zwana dalej Instrukcją, jest dokumentem wewnętrznym wydanym przez Burmistrza Gminy i Miasta Susz i ma zastosowanie do przetwarzania danych osobowych w systemach informatycznych Urzędu Gminy i Miasta Susz, w celu bezpiecznego ich wykorzystywania.

§ 2.

1. Instrukcja określa ogólne zasady i tryb postępowania Administratora Danych Osobowych, osób wyznaczonych przez niego oraz wszystkich użytkowników, przetwarzających dane osobowe w systemach informatycznych Urzędu Gminy i Miasta Susz.
2. Instrukcja została opracowana zgodnie z wymogami § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. nr 100, poz. 1024).

§ 3.

Określenia i skróty użyte w Instrukcji oznaczają:

1. **Administrator Danych Osobowych** – Burmistrz Gminy i Miasta Susz, zwany dalej **Administratorem**.
2. **Administrator Bezpieczeństwa Informacji, zwany dalej ABI** – osoba wyznaczona przez Administratora lub osobę upoważnioną przez niego, odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemów oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w tych systemach oraz odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych, w których przetwarzane są dane osobowe.
3. **Osoba upoważniona lub użytkownik systemu, zwany dalej użytkownikiem** – osoba posiadająca upoważnienie wydane przez Administratora lub osobę wyznaczoną przez niego i dopuszczona, w zakresie w nim wskazanym, jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej.
4. **Przełożony użytkownika, zwany dalej przełożonym** – kierownik komórki organizacyjnej Urzędu Gminy i Miasta Susz lub bezpośredni przełożony.
5. **Osoba trzecia** – to każda osoba nieupoważniona i przez to nieuprawniona do dostępu do danych osobowych zbiorów będących w posiadaniu Administratora. Osobą trzecią jest również osoba posiadająca upoważnienie wydane przez Administratora podejmująca czynności w zakresie przekraczającym ramy jego upoważnienia.
6. **System informatyczny**, zwany dalej systemem to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
7. **Zabezpieczenie systemu informatycznego** – wdrożenie przez Administratora stosownych środków organizacyjnych i technicznych w celu zabezpieczenia zasobów oraz ochrony danych przed dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem przez osobę trzecią.
8. **Przetwarzanie danych osobowych** – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, zmienianie, udostępnianie i ich usuwanie.

§ 4.

1. ABI może zlecić innej osobie, zatrudnionej u Administratora wykonywanie określonych czynności, leżących w zakresie jego obowiązków.
2. Kontrola prawidłowości wykonywania czynności o których mowa w ust. 1 należy do ABI.
3. Osoba, o której mowa w ust. 1 niezwłocznie informuje ABI o podjętych przez siebie czynnościach.

Rozdział 2
Przydział haseł i identyfikatorów dla użytkowników.

§ 5.

Systemy, w których przetwarza się dane osobowe w zbiorach Urzędu Gminy i Miasta Susz muszą być wyposażone w mechanizmy uwierzytelnienia użytkownika oraz kontroli dostępu do nich.

§ 6.

1. Hasła dostępu opracowuje się indywidualnie dla każdego uprawnionego użytkownika systemu i natychmiast zmienia w wypadku podejrzenia lub stwierdzenia ujawnienia ich osobom trzecim.
2. Hasła dostępu zapisywane są na ekranie monitora w formie niejawnej i mogą być znane tylko użytkownikowi oraz ABI.
3. Hasła obowiązują 1 rok i zmienia je ABI w pierwszym tygodniu nowego roku kalendarzowego lub wg wymagań aplikacji systemowych.
4. Osobą odpowiedzialną za techniczny sposób ustalania, przechowywania i wprowadzania haseł jest ABI lub użytkownik dla haseł, których zmiana jest okresowo wymuszana przez aplikacje systemowe.

§ 7.

1. Identyfikatory dla użytkowników przydziela ABI. Identyfikator po wylogowaniu danej osoby z systemu, nie może być przydzielony innemu użytkownikowi.
2. Identyfikator wpisuje się do „Ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych".

§ 8.

1. Użytkownik ponosi odpowiedzialność za czynności wykonywane w systemie przy użyciu identyfikatora i hasła, którymi się posługuje lub posługiwał.
2. Użytkownik zobowiązany jest do utrzymania haseł dostępu w tajemnicy, a w szczególności do dołożenia starań, w celu uniemożliwienia zapoznania się z nimi osób trzecich, nawet po ustaniu ich ważności.

Rozdział 3
Rejestrowanie i wyrejestrowywanie użytkowników.

§ 9.

1. Rejestracji i wyrejestrowania użytkowników w systemie dokonuje ABI na podstawie informacji uzyskanej od przełożonego użytkownika, wprowadzając dane do ewidencji, o której mowa § 7 ust. 2.
2. Ewidencja zawierać powinna:
   - imię i nazwisko użytkownika;

- nazwę komórki organizacyjnej, w której jest zatrudniony;
- identyfikator i hasło użytkownika;
- datę nadania uprawnień;
- datę odebrania uprawnień.

3. Jakakolwiek zmiana informacji wyszczególnionych w ewidencji podlega natychmiastowemu odnotowaniu.

§ 10.

1. Zarejestrowanie użytkownika w systemie wymaga spełnienia następujących warunków:
   1) złożenie wniosku przez przełożonego do Administratora lub osoby przez niego upoważnionej według wzoru zawartego w załączniku nr 1 do Instrukcji;
   2) udzielenie wskazanej osobie dostępu do przetwarzania danych osobowych;
   3) podpisanie przez osobę, ubiegającą się o dostęp, oświadczenia dotyczącego zapoznania się z przepisami o ochronie danych osobowych i zobowiązania do zachowania w tajemnicy informacji związanych z ich przetwarzaniem, według wzoru zawartego w załączniku nr 2 do Instrukcji;
2. Z chwilą zarejestrowania w systemie użytkownik jest informowany przez ABI o ustalonym dla niego identyfikatorze i obowiązku posługiwania się hasłem dostępu.
3. Dokumenty, o których mowa w ust. 1 podlegają przechowaniu:
   1) wniosek przełożonego o udzielenie dostępu osobie w dokumentacji adresata;
   2) oryginał oświadczenia osoby ubiegającej się o dostęp w komórce kadrowej, a kopia oświadczenia w dokumentacji ABI;
   3) oryginał upoważnienia o dostępie otrzymuje osoba upoważniona, a kopie trafiają do akt personalnych pracownika i dokumentacji ABI.

§ 11.

1. Użytkownika wyrejestrowuje się z systemu na wniosek przełożonego - po utracie uprawnień dostępu do przetwarzania danych, co może mieć miejsce w sytuacjach:
   1) ustania zatrudnienia użytkownika u Administratora;
   2) zmiany zakresu obowiązków użytkownika.
2. Rozwiązanie umowy o pracę powoduje utratę dostępu do przetwarzania danych i natychmiastowe wyrejestrowanie użytkownika z systemu, wykreślenie identyfikatora z ewidencji oraz unieważnienie jego hasła i identyfikatora.
3. Przełożeni użytkowników zobowiązani są do przekazywania pisemnie informacji ABI w przypadku zaistnienia okoliczności, o których mowa w ust. 1 i 2.

Rozdział 4
Procedury rozpoczęcia i zakończenia pracy w systemie.

§ 12.

1. Użytkownik rozpoczynający pracę zobowiązany jest przestrzegać procedur, które mają na celu sprawdzenie zabezpieczenia pomieszczenia, w którym przetwarzane są dane osobowe, swojego stanowiska pracy oraz stanu sprzętu komputerowego, a w szczególności:
   1) przed wejściem do pomieszczenia sprawdzić czy na drzwiach i zamkach nie ma widocznych śladów prób niepowołanego ich otwierania;

2) sprawdzić stan okien i krat oraz ocenić czy w pomieszczeniu nie ma znaków wskazujących na pobyt w nim osób nieuprawnionych;
3) sprawdzić stan sprzętu informatycznego oraz zamknięcie szaf i biurek;
4) po włączeniu komputera ocenić jakość jego pracy i stwierdzić zmiany.

2. Użytkownik przed przystąpieniem do przetwarzania danych powinien zalogować się w systemie, posługując się swoim identyfikatorem i hasłem. Po zalogowaniu się należy ocenić pracę systemu i stan zbioru danych.
3. Użytkownik w czasie pracy powinien stosować przedsięwzięcia zapewniające bezpieczeństwo przetwarzania danych osobowych w systemie:
   1) ustawić ekrany monitorów w pomieszczeniach tak, aby uniemożliwiać podgląd osób nieuprawnionych;
   2) dopilnować aby w pomieszczeniach, stanowiących obszar przetwarzania danych osobowych przebywały osoby trzecie, tylko za zgodą przełożonych i w obecności osób uprawnionych;
   3) stosować urządzenia zabezpieczające przed utratą danych, spowodowaną awarią zasilania lub zakłóceniami w sieci elektrycznej. Potrzeby w tym zakresie zgłaszają ABI - przełożeni użytkownika;
   4) stosować wygaszacze ekranów, które włączają się po upływie 3 minut bezczynności komputera.
4. Po zakończeniu pracy użytkownik powinien przestrzegać następujących zasad:
   1) wylogować się z systemu i zaczekać na jego wyłączenie się;
   2) sprawdzić czy nie zostały pozostawione bez nadzoru nośniki informacji;
   3) upewnić się, że szafy i biurka z dokumentacją są zamknięte;
   4) wyłączyć odbiorniki energii elektrycznej, zamknąć pomieszczenie i klucze oddać w wyznaczone miejsce.
5. Po godzinach pracy Administrator lub osoba upoważniona przez niego zapewnia monitorowanie lub fizyczną ochronę pomieszczeń, w których przetwarzane są dane osobowe.

§ 13.

Pomieszczenia, w których przetwarzane są dane osobowe w zbiorach zarejestrowanych u Generalnego Inspektora Ochrony Danych Osobowych oraz zbiorach danych personalnych i finansowych - pracowników zatrudnionych przez Administratora, powinny być zabezpieczone, a deponowane klucze ewidencjonowane.

§ 14.

1. W przypadku stwierdzenia przez użytkownika prób niepowołanego naruszenia zabezpieczenia fizycznego pomieszczenia, zmian w systemie bezpieczeństwa systemu lub zauważenia, że stan urządzeń, zawartość zbiorów danych, ujawnione metody pracy lub sposób działania programu mogą wskazywać na naruszenie danych osobowych – postępuje zgodnie z „Instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Gminy i Miasta Susz”, która stanowi załącznik nr 5 do niniejszej instrukcji.
2. Rozpoczynając pracę użytkownik powinien zwrócić szczególną uwagę na okoliczności, o których mowa w ust. 1 i przypadku ich zaistnienia natychmiast informować ABI i przełożonego.

Rozdział 5
Tworzenie i przechowywanie kopii awaryjnych.

§ 15.

1. Kopie awaryjne tworzy i przechowuje ABI.
2. Kopie awaryjne należy wykonywać w każdy piątek tygodnia i na koniec każdego miesiąca. Przełożony może polecić codzienne wykonywanie kopii awaryjnych.
3. Kopie awaryjne należy tworzyć na odpowiedniej jakości nośnikach informacji, które należy szczegółowo opisać i przechowywać zgodnie z przepisami.

§ 16.

1. Kopiowanie danych osobowych na nośniki informacji oraz robienie wydruków jest zabronione chyba, że istnieje konieczność ich sporządzania, która wynika z nałożonych na użytkownika obowiązków i dozwolona jest przepisami prawa.
2. Wykorzystywanie nośników informacji lub wydruków w innym celu niż wskazany w ust. 1 jest zabronione.

§ 17.

1. Czas przechowywania kopii awaryjnych, jeżeli nie stanowią inaczej przepisy prawa, należy ograniczyć do:
   1) codziennych – 1 tydzień;
   2) tygodniowych – 1 miesiąc;
   3) miesięcznych – 1 rok.
2. Kopie awaryjne należy przechowywać w innych pomieszczeniach niż zbiory danych osobowych.
3. Kopie awaryjne przechowuje użytkownik w miejscach wskazanych przez przełożonego, zapewniających im odpowiednie warunki bezpieczeństwa.

§ 18.

1. ABI, po upływie roku, sprawdza kopie awaryjne i określa ich przydatność do wykorzystania w wypadku awarii systemu.
2. Zdezaktualizowane i uszkodzone kopie awaryjne należy mechanicznie niszczyć w sposób uniemożliwiający ich ponowne użycie.
3. Nie wolno sporządzać wydruków z kopii awaryjnych i innych nośników informacji, które podlegają zniszczeniu.

Rozdział 6
Ochrona systemu informatycznego przed wirusami komputerowymi.

§ 19.

1. Użytkownik ma obowiązek na bieżąco sprawdzać obecność wirusów komputerowych. Czynność ta powinna być zaprogramowana w systemie, który automatycznie sygnalizuje obecność wirusów, w trakcie włączania systemu lub wprowadzania danych z zewnętrznych nośników informacji.
2. Kontrola antywirusowa systemu obejmować powinna wszystkie nośniki magnetyczne i optyczne, służące zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.

3. Obowiązkiem ABI jest dostarczanie, uaktualnianie i instalowanie nowego oprogramowania antywirusowego.

Rozdział 7
Przechowywanie nośników informacji, w tym kopii informatycznych i wydruków.

§ 20.

1. Nośniki informacji, w tym kopie informatyczne i wydruki komputerowe przechowuje się wyłącznie wówczas, gdy jest to konieczne i dozwolone przepisami prawa.
2. Nośniki informacji, w tym wydruki komputerowe przechowuje się w wyznaczonych pomieszczeniach w szafach i innych meblach biurowych, które posiadają odpowiednie zamknięcia, uniemożliwiające niepowołany dostęp do nich osób trzecich.
3. Pomieszczenia, o których mowa w ust. 2 winny spełniać określone warunki bezpieczeństwa, a w szczególności posiadać:
   1) wewnętrzne ściany, gwarantujące trwałe oddzielenie ich od innych pomieszczeń;
   2) pełne drzwi wejściowe, zaopatrzone w co najmniej jeden zamek o skomplikowanym mechanizmie otwierania;
   3) odpowiednie zabezpieczenie okien przed dostępem z zewnątrz i obserwacją;
4. W razie uzasadnionej potrzeby ABI wprowadza dalej idące środki bezpieczeństwa dotyczące przechowywania nośników informacji w szafach i innych meblach biurowych, które winny być:
   1) zaopatrzone w co najmniej jeden zamek o skomplikowanym mechanizmie otwierania, tj. w szczególności zamek patentowy lub szyfrowy;
   2) po zakończeniu pracy zamknięte i opieczętowane.

Rozdział 8
Przeglądy i konserwacje systemów oraz zbiorów danych osobowych.

§ 21.

1. Okresowe przeglądy i konserwacje sprzętu komputerowego, wynikające z eksploatacji, warunków zewnętrznych oraz ważności systemów dla funkcjonowania Urzędu Gminy i Miasta Susz, wykonuje ABI lub osoba upoważniona przez Administratora.
2. Bieżącą konserwację i naprawę sprzętu wykonuje ABI lub osoba upoważniona przez Administratora.
3. Urządzenia, dyski lub inne informatyczne nośniki informacji, przeznaczone do napraw w autoryzowanych firmach zewnętrznych, pozbawia się przed naprawą zapisu danych osobowych albo naprawia się je pod nadzorem ABI.

§ 22.

1. Urządzenia, dyski lub inne informatyczne nośniki informacji, zawierające zapis danych osobowych przeznaczone do likwidacji należy pozbawić zapisu, a w przypadku, gdy nie jest to możliwe, uszkodzić mechanicznie w sposób uniemożliwiający ich odczytanie.
2. Urządzenia, dyski lub inne informatyczne nośniki informacji, zawierające zapis danych osobowych przeznaczone do przekazania innemu podmiotowi, który nie jest uprawniony do otrzymania takich danych, należy wcześniej pozbawić zapisów danych - postępując zgodnie z ust. 3 § 21.

Rozdział 9
Postępowanie w zakresie komunikacji w sieci komputerowej.

§ 23.

1. Komunikacja w sieci komputerowej jest dozwolona tylko po odpowiednim zalogowaniu się i podaniu indywidualnego hasła użytkownika.
2. Wprowadzanie do systemu informacji z zewnątrz jest dopuszczalne tylko przy stwierdzeniu legalności i wiarygodności źródeł informacji i przez użytkownika posiadającego uprawnienia, wynikające z zakresu jego obowiązków.
3. Uprawnienia, o których mowa w ust. 1 nadaje ABI na wniosek przełożonego użytkownika.

§ 24.

Pomieszczenie, w którym znajdują się serwery systemów, powinno być wydzielone wyłącznie dla potrzeb systemów informatycznych znajdować się na piętrze budynku, posiadać wentylację wymuszoną oraz spełniać warunki zawarte w § 20 ust. 3 i 4. Dostęp do ww. pomieszczenia powinien mieć wyłącznie ABI oraz osoby upoważnione przez Administratora.

Rozdział 10
Postanowienia końcowe.

§ 25.

1. Instalację nowego oprogramowania systemowego oraz oprogramowania użytkowego, gwarantującego bezpieczeństwo przetwarzania danych osobowych wykonuje ABI lub osoba upoważniona przez Administratora.
2. ABI prowadzi „Rejestr zbiorów danych osobowych przetwarzanych w systemach informatycznych".
3. ABI dokonuje sprawdzenia sprawności funkcjonowania zabezpieczeń systemów, w których przetwarzane są dane osobowe, nie rzadziej niż raz na rok.

§ 26.

1. Każdy pracownik zatrudniony przy przetwarzaniu danych osobowych w systemie, zobowiązany jest zapoznać się z niniejszą Instrukcją i stosować jej przepisy na swoim stanowisku pracy.
2. Nadużycie przez użytkownika postanowień niniejszej Instrukcji, może stanowić podstawę do pociągnięcia go do odpowiedzialności przewidzianej właściwymi przepisami prawa.

§ 27.

W sprawach nie uregulowanych niniejszą Instrukcją zastosowanie znajdują przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101 poz. 926 ze zm.) i rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. nr 100, poz. 1024).

Załącznik Nr 1 do „Instrukcji określającej sposób zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych”

…..... Susz, dn. .....
(pieczęć komórki organizacyjnej)

Administrator Danych Osobowych
Urzędu Gminy i Miasta Susz

Na podstawie § 10 ust. 1 (§ 11 ust. 1)* „Instrukcji określającej sposób zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych w Urzędzie Gminy i Miasta Susz, wnioskuję o udzielenie (pozbawienie)*

Pani/Panu/Pana* .....

dostępu do przetwarzania danych osobowych w komórce organizacyjnej Urzędu Gminy i Miasta Susz z powodu: /przyjęcia do pracy, przejścia na inne stanowisko, zwolnienia z pracy/* lub innego (jakiego?):
…..

1. Nazwa zbioru danych osobowych .....
2. Uprawnienia: (użytkownika systemu)* - (rozpatrywania wniosków)* z tytułu zajmowanego stanowiska (jakiego?) …….
3. Sposób przetwarzania danych osobowych: papierowy/ informatyczny/*
4. Miejsce przetwarzania (adres siedziby) .....
   danych osobowych (piętro, nr pokoju) .....
5. Zobowiązano pracownika do zapoznania się i do podpisania oświadczenia o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych: tak/ nie*

.....
(podpis i pieczątka)

/* niepotrzebne skreślić

Załącznik Nr 2 do „Instrukcji określającej sposób zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych”

.....
(imię i nazwisko pracownika)

.....
(stanowisko i nazwa komórki organizacyjnej)

O Ś W I A D C Z E N I E

Oświadczam, że zapoznałem się z przepisami dotyczącymi ochrony danych osobowych i zobowiązuję się do przestrzegania:

1. Ustawy z dni 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz.U. z 2002 r. Nr 101 poz. 926 z późn. zm.).
2. Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. nr 100, poz. 1024).
3. Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy i Miasta Susz.
4. Instrukcji określającej sposób zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych w Urzędzie Gminy i Miasta Susz.

Jednocześnie w czasie wykonywania swoich obowiązków służbowych zobowiązuję się do:

1) zapewnienia ochrony danym osobowym przetwarzanym w zbiorach Urzędu Gminy i Miasta Susz, a w szczególności zapewnienia ich bezpieczeństwa przed udostępnianiem osobom trzecim i nieuprawnionym, zabraniem, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem,
2) zachowaniem w tajemnicy, także po ustaniu stosunku pracy, wszelkich informacji dotyczących funkcjonowania systemów lub urządzeń służących do przetwarzania danych osobowych w zbiorach Urzędu Gminy i Miasta Susz,
3) zachowania w tajemnicy hasła dostępu do systemów informatycznych, przetwarzających dane osobowe w Urzędzie Gminy i Miasta Susz, również po upływie jego ważności,
4) natychmiastowego zgłaszania przełożonemu i Administratorowi Bezpieczeństwa Informacji stwierdzenia, na swoim stanowisku pracy, próby lub faktu naruszenia zabezpieczenia fizycznego pomieszczenia, bezpieczeństwa zbioru lub systemu informatycznego, w którym przetwarzane są dane osobowe.

.....
(podpis pracownika ubiegającego się o dostęp)

Susz, dnia .....

Oświadczenie wypełnia tylko pracownik, który wykonując swoje obowiązki służbowe, powinien mieć dostęp do przetwarzania danych osobowych. Oświadczenie jest niezbędne do realizacji zapisu art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

Załącznik nr 3 do zarządzenia nr 42/2008
Burmistrza GiM Susz z dnia 6 maja 2008 r.

INSTRUKCJA
postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Gminy i Miasta Susz

Spis treści:

Rozdział 1
Postanowienia ogólne

§ 1.

1. Instrukcja określa tryb postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych lub powzięcia podejrzenia o takim naruszeniu.
2. Niniejsza Instrukcja, jest wewnętrznym dokumentem wydanym przez Burmistrza Gminy i Miasta Susz i przeznaczona jest dla osób zatrudnionych przy przetwarzaniu danych osobowych.
3. Przestrzeganie postanowień niniejszej Instrukcji służyć ma wykrywaniu i właściwemu reagowaniu na przypadki naruszenia ochrony danych osobowych w Urzędzie Gminy i Miasta Susz.

§ 2.

Określenia i skróty użyte w Instrukcji oznaczają:

1. **Administrator Danych Osobowych** – Burmistrz Gminy i Miasta Susz, zwany dalej Administratorem (ADO).
2. **Administrator Bezpieczeństwa Informacji,** zwany dalej **ABI** – osoba wyznaczona przez Administratora lub osobę upoważnioną, odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych Urzędu Gminy i Miasta Susz, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemów oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w tych systemach oraz odpowiedzialna za sprawność, konserwacje i wdrażanie technicznych zabezpieczeń systemów informatycznych, w których przetwarzane są dane osobowe w zbiorach komórek organizacyjnych Urzędu Gminy i Miasta Susz.
3. **Osoba upoważniona lub użytkownik systemu,** zwany dalej **użytkownikiem** – osoba posiadająca upoważnienie wydane przez Administratora lub osobę upoważnioną przez niego i dopuszczona w zakresie w nim wskazanym, jako użytkownik do przetwarzania danych osobowych w systemie informatycznym komórki organizacyjnej Urzędu Gminy i Miasta Susz.
4. **Przełożony użytkownika,** zwany dalej **przełożonym** – kierownik komórki organizacyjnej Urzędu Gminy i Miasta Susz lub bezpośredni przełożony.
5. **System informatyczny,** zwany dalej **systemem** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
6. **Zabezpieczenie systemu informatycznego** – wdrożenie przez Administratora stosownych środków organizacyjnych i technicznych w celu zabezpieczenia zasobów oraz ochrony danych przed dostępem, modyfikacją ujawnieniem, pozyskaniem lub zniszczeniem przez osobę trzecią.
7. **Przetwarzanie danych osobowych** – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, udostępnianie i usuwanie, a zwłaszcza tych, które są wykonywane w systemach informatycznych.

§ 3.

1. **Naruszenie ochrony danych osobowych, może być spowodowane:**
   1) niewłaściwym oddziaływaniem czynników zewnętrznych, takich jak: temperatura otoczenia, wilgotność, pole elektromagnetyczne, wirusy komputerowe, skutki powodzi, pożaru, itp.;
   2) niekontrolowanym działaniem osób trzecich, powodującym zakłócenia systemu podczas włamania, niewłaściwym działaniem zespołów serwisowych, przetwarzaniem danych osobowych bez uprawnień, tworzeniem w zbiorach użytkownika nieautoryzowanych kont dostępu;

3) umyślnym lub nieumyślnym działaniem, a nawet zaniechaniem działania użytkowników przetwarzających dane osobowe.

2. **Za naruszenie ochrony danych osobowych uważa się w szczególności:**
   1) brak możliwości fizycznego dostępu do danych np. zagubiony klucz do pomieszczenia, lub mebli biurowych, w których przechowywane są dokumenty, zniszczona szafa z dokumentami, brak nośników informacji, zalane pomieszczenie, brak sprzętu komputerowego itp.;
   2) brak dostępu do zawartości zbioru danych – zbiór istnieje lecz nie można go otworzyć;
   3) zmienioną zawartość zbioru, niepoprawną treść, postać, data, różnicę w danych itp.;
   4) próbę lub fakt nieuprawnionego dostępu do zbioru danych lub pomieszczenia w którym jest przetwarzany np. zmiana ułożenia kolejności dokumentów, otwarte drzwi lub meble biurowe, nietypowe ustawienie sprzętu lub pojawienie się nowych dokumentów;
   5) różnicę funkcjonowania systemu, a w szczególności wyświetlania komunikatów i informacji o błędach oraz nieprawidłowościach w wykonywaniu operacji;
   6) zniszczenie lub próby zniszczenia, w sposób nieautoryzowany danych ze zbioru lub danych systemowych;
   7) zmianę lub utratę danych zapisanych na kopiach awaryjnych lub zapisach archiwalnych;
   8) nieskuteczne niszczenie nośników informacji zawierających dane osobowe (dyskietki, nośniki optyczne, wydruki papierowe), umożliwiające ponowny ich odczyt przez osoby nieuprawnione;
   9) próba nielegalnego logowania się do systemu lub włamania do systemu;
   10) zmienione oprogramowanie systemu, stwierdzone przez użytkownika po przerwie w przetwarzaniu danych.
3. Niniejszą Instrukcję stosuje się także w przypadku stwierdzenia, że stan pomieszczeń i szaf, bądź mebli biurowych, w których przechowuje się dokumentację lub zawartości tej dokumentacji wzbudzają podejrzenie, że dostęp do nich mogły mieć osoby trzecie.

Rozdział 2
Zabezpieczenie przed naruszeniem obszaru przetwarzania danych osobowych

§ 4.

1. Dane osobowe przetwarza się w pomieszczeniach lub częściach pomieszczeń Urzędu Gminy i Miasta Susz, ul. Wybickiego 6.
2. Przebywanie osób nieuprawnionych wewnątrz obszaru, w którym są przetwarzane dane jest możliwe tylko w obecności użytkownika i za zgodą przełożonego.
3. Budynki lub pomieszczenia, w których przetwarzane są dane, powinny być zamykane na czas nieobecności użytkowników, w sposób uniemożliwiający do nich dostęp osób trzecich.

§ 5.

Zabezpieczenie systemu informatycznego, w zakresie nieuwzględnionym w niniejszej Instrukcji, reguluje „Instrukcja określająca sposób zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych w Urzędzie Gminy i Miasta Susz”.

Rozdział 3
Kontrola przestrzegania zasad zabezpieczenia systemu ochrony danych osobowych

§ 6.

1. Codzienną kontrolę w zakresie ochrony danych osobowych sprawuje użytkownik.
2. Nadzór nad przestrzeganiem zasad ochrony danych osobowych w komórce organizacyjnej sprawuje przełożony.
3. ABI sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych, przetwarzanych w systemach informatycznych i określonych niniejszą Instrukcją oraz dokonuje stałych kontroli i oceny funkcjonowania mechanizmów technicznych zabezpieczeń systemów, w których przetwarzane są dane osobowe.

Rozdział 4
Postępowanie w przypadku naruszenia zabezpieczenia systemu ochrony danych osobowych

§ 7.

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie systemu ochrony, o których mowa w § 3 niniejszej Instrukcji, użytkownik zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie przełożonego oraz ABI lub osobę upoważnioną przez ABI.

§ 8.

Użytkownik do momentu przybycia ABI, lub osoby przez niego upoważnionej powinien:

1) zabezpieczyć dostęp do pomieszczenia lub urządzenia;
2) powstrzymać się od rozpoczęcia lub kontynuowania jakichkolwiek czynności mogących spowodować zatarcie śladów, bądź dowodów naruszenia ochrony;
3) zatrzymać pracę na komputerze, na którym zaistniało naruszenie ochrony oraz nie uruchamiać innych urządzeń, które mogą mieć związek z naruszeniem ochrony;
4) podjąć, stosownie do zaistniałej sytuacji działania, które zapobiegną ewentualnej utracie danych osobowych.

§ 9.

1. ABI po otrzymaniu informacji o naruszeniu lub próby naruszenia zabezpieczenia systemu przetwarzającego dane osobowe, podejmuje działania zmierzające do usunięcia powstałego zagrożenia.
2. Po przybyciu na miejsce, o którym mowa w ust. 1, ABI realizuje czynności w kolejności:
   1) ocenia sytuację, uwzględniając stan pomieszczenia, w którym przetwarzane są dane, stan urządzenia i zbioru oraz identyfikuje zakres negatywnych następstw naruszenia ochrony danych osobowych;
   2) wysłuchuje relacji użytkownika lub osoby, która dokonała powiadomienia;
   3) podejmuje działania mające na celu ustalenie sprawcy, miejsca, czasu i sposobu dokonania naruszenia ochrony;
   4) w zależności od zakresu naruszenia ochrony podejmuje decyzje o dalszym postępowaniu, wydając użytkownikowi stosowne polecenia i wskazówki do obsługi urządzeń;

5) biorąc pod uwagę skalę oraz skutki naruszenia ochrony, ABI decyduje o powołaniu doraźnego zespołu i powiadomieniu o zdarzeniu Administratora lub osobę upoważnioną przez niego.

§ 10.

1. ABI z przebiegu zdarzenia sporządza notatkę służbową, która obejmuje:
   1) dane osoby stwierdzającej naruszenie ochrony;
   2) datę, godzinę i miejsce naruszenia ochrony;
   3) rodzaj naruszenia ochrony;
   4) czas powiadomienia o zdarzeniu;
   5) opis podjętych czynności;
   6) wnioski do realizacji.
2. Notatkę, o której mowa w ust. 1, ABI przekazuje Administratorowi lub osobie upoważnionej przez niego.

§ 11.

Zgodę na ponowne uruchomienie komputera lub innych urządzeń oraz kontynuowanie przetwarzania danych, wyraża ABI lub osoba przez niego upoważniona.

§ 12.

Dokonywanie zmian w miejscu naruszenia ochrony bez zgody, o której mowa w § 11 jest dopuszczalne tylko w wypadku konieczność ratowania osób, mienia albo zapobiegania powstaniu innego niebezpieczeństwa.

§ 13.

1. W przypadku powołania doraźnego zespołu, o którym mowa w § 9, pracą jego kieruje ABI.
2. Zespół z przeprowadzonych czynności sporządza protokół, w którym ujmuje skalę stwierdzonych naruszeń ochrony, przyczyny ich powstania oraz skutki, jakie wpłynęły lub wpłynąć mogą na stan zabezpieczenia i ochrony danych osobowych.
3. Protokół zawierać powinien wnioski określające zakres działań organizacyjnych i technicznych, zapobiegających w przyszłości naruszeniom ochrony danych osobowych.
4. Protokół przekazywany jest Administratorowi lub osobie upoważnionej przez niego w celu akceptacji wniosków i zaleceń usprawniających zabezpieczenia ochrony danych.

§ 14.

W przypadku stwierdzenia:

1) błędu użytkownika systemu – ABI przeprowadza dodatkowe szkolenie osób zatrudnionych przy przetwarzaniu danych w komórce organizacyjnej;
2) uaktywnienia wirusa – należy zgłosić ABI, który ustali źródło jego pochodzenia oraz uaktualni zabezpieczenia antywirusowe;
3) zaniedbania ze strony użytkownika – należy w stosunku do niego zastosować konsekwencje wynikające z właściwych przepisów prawa;
4) włamania, w celu nielegalnego pozyskania danych – należy dokonać szczegółowej analizy wdrożonych środków zabezpieczenia i zapewnić skuteczniejszą ochronę oraz powiadomić Administratora;
5) złego stanu urządzenia lub złego działania programu – należy niezwłocznie powiadomić ABI i przeprowadzić kontrolę czynności serwisowo-programowych.

Rozdział 5
Postanowienia końcowe

§ 15.

1. Każdy użytkownik przetwarzający dane osobowe w zbiorach Urzędu Gminy i Miasta Susz zobowiązany jest zapoznać się z niniejszą Instrukcją i stosować przepisy w niej zawarte na swoim stanowisku pracy.
2. Nadużycie przez użytkownika postanowień niniejszej Instrukcji może stanowić podstawę do pociągnięcia go do odpowiedzialności dyscyplinarnej, odszkodowawczej lub karnej, w trybie i na zasadach przewidzianych przepisami prawa.

§ 16.

W sprawach nie uregulowanych niniejszą Instrukcją zastosowanie znajdują przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.) i rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. nr 100, poz. 1024).