Zarządzenie Nr Or.0153-196/10
Wójta Gminy Dąbrówno
z dnia 23 lutego 2010 r.

w sprawie wdrożenia do stosowania w Urzędzie Gminy Dąbrówno „Polityki bezpieczeństwa Urzędu Gminy Dąbrówno" i „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Dąbrówno".

Na podstawie art. 26 i 36 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 § 3, 4 i 5 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) **z a r z ą d z a m,** co następuje:

§ 1

Wprowadzam „Politykę bezpieczeństwa Urzędu Gminy Dąbrówno" i „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Dąbrówno" do stosowania i bezwzględnego przestrzegania przez pracowników Urzędu Gminy Dąbrówno, zgodnie z załącznikiem Nr 1 i 2 niniejszego zarządzenia.

§ 2

Zobowiązuję wszystkich pracowników Urzędu do zapoznania się w terminie do 31 maja 2010 r. z treścią „Polityki bezpieczeństwa Urzędu Gminy Dąbrówno" i „Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Dąbrówno". Fakt ten należy potwierdzić własnoręcznym podpisem w stosownym wykazie.

§ 3

Wykonanie zarządzenia powierza się Sekretarzowi Gminy i informatykowi Urzędu.

§ 4

Zarządzenie wchodzi w życie z dniem podjęcia.

W Ó J T
Tadeusz Błaszkiewicz

Załącznik Nr 1
do Zarządzenia Nr Or. 0153-196/10
Wójta Gminy Dąbrówno
z dnia 23 lutego 2010 r.

POLITYKA BEZPIECZEŃSTWA URZĘDU GMINY DĄBRÓWNO

W celu zabezpieczenia danych gromadzonych i przetwarzanych w Urzędzie Gminy w Dąbrównie oraz jego systemie informatycznym, a w szczególności w celu ochrony danych osobowych, wprowadza się określone w niniejszym dokumencie zasady bezpieczeństwa.

Mając świadomość, że żadne zabezpieczenie techniczne nie gwarantuje 100%-towej szczelności systemu, konieczne jest aby każdy użytkownik systemu pełen świadomej odpowiedzialności, postępował zgodnie z przyjętymi zasadami i minimalizował zagrożenia wynikające z błędów ludzkich.

Rozdział I. Podstawa prawna

§ 1

1. Niniejszy dokument został opracowany na podstawie:
   1) Ustawy z dnia 29 sierpnia 1997 r o ochronie danych osobowych (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, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

Rozdział II. Postanowienia ogólne

§ 2

1. Ilekroć mowa w niniejszym dokumencie o:
   1) **Polityce** – należy przez to rozumieć „Politykę Bezpieczeństwa Urzędu Gminy w Dąbrównie",
   2) **Urzędzie** – należy przez to rozumieć Urząd Gminy w Dąbrównie,
   3) **Wójcie** – należy przez to rozumieć Wójta Gminy Dąbrówno.

§ 3

Administratorem danych osobowych zawartych i przetwarzanych w systemie informatycznym Urzędu oraz tradycyjnie w formie papierowej jest Wójt.

§ 4

Administrator danych osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemie informatycznym Urzędu. W celu zrealizowania tych obowiązków administrator danych wprowadza Politykę bezpieczeństwa jako dokument obowiązujący w Urzędzie.

Rozdział III. Zagadnienia organizacyjne

§ 5

1. Wójt wyznacza Administratora bezpieczeństwa informacji i Administratora systemu informacyjnego. W związku z faktem, iż w części zadania Administratora bezpieczeństwa informacji i Administratora systemu informacji pokrywają się dopuszcza się możliwość wyznaczenia na te stanowiska jednej osoby.
2. Do Kierownictwa Urzędu należy zapewnienie odpowiednich pomieszczeń, stosownie zabezpieczonych i wyposażonych do przetwarzania i przechowywania danych osobowych, zaznajomienie pracowników z prawnymi oraz pracowniczymi konsekwencjami naruszenia bezpieczeństwa danych osobowych.
3. Pracownicy upoważnieni do przetwarzania danych osobowych w systemie informatycznym jak i ręcznym, zobowiązani są do zapoznania się i przestrzegania Polityki.
4. Osoba przetwarzająca dane osobowe składa oświadczenie o zapoznaniu się z przepisami i odpowiedzialnością karną za naruszenie ochrony danych osobowych oraz zachowaniu tajemnicy, którego wzór stanowi załącznik nr 1 do Polityki.
5. Fakt zapoznania się z Polityką pracownik potwierdza własnoręcznym podpisem na stosownym wykazie, którego wzór stanowi załącznik nr 2 do Polityki.
6. Pracownikom wolno przebywać na terenie Urzędu tylko w godzinach ich pracy, a po godzinach pracy – po zawiadomieniu i uzyskaniu zgody bezpośredniego przełożonego.
7. Korzystanie z systemu informatycznego służącego do przetwarzania danych osobowych może odbywać się tylko w godzinach pracy, a po godzinach pracy – po zawiadomieniu i uzyskaniu zgody bezpośredniego przełożonego.

§ 6

Wszystkie zbiory danych osobowych dla których Administratorem jest Wójt, znajdują się w budynku Urzędu Gminy Dąbrówno, ul. Kościuszki 21,. 14-120 Dąbrówno. Szczegółowy wykaz zbiorów danych osobowych, zawierający: nazwę zbioru, formę ich przetwarzania, nazwę oprogramowania i jego producenta oraz nr pokoju w którym się znajduje, stanowi załącznik nr 3 do Polityki.

Rozdział IV. Sposób przepływu danych

§ 7

1. Stacje robocze w Urzędzie połączone są w sieć logiczną za pośrednictwem sieci LAN.
2. W systemie informatycznym Urzędu występuje jeden serwer pełniący rolę bazodanowego w przypadku konieczności przetwarzania większych zbiorów lub udostępniania na więcej niż jednej stacji roboczej.
3. Serwer znajduje się w pomieszczeniu do którego nie ma bezpośredniego wejścia z korytarza. Wejście do serwerowi jest z pokoju nr 8. Pomieszczenie to znajduję się na pierwszym piętrze

Rozdział IV. Zabezpieczenia fizyczne

§ 8

1. Wejścia do Urzędu zabezpieczone winny być przynajmniej dwoma zamkami drzwiowymi; a okna na parterze budynku kratami.
   Do budynku Urzędu można dostać się wejściami:
   1) głównym, od frontu budynku po prawej stronie, chronionymi wejściowymi drzwiami antywłamaniowymi zamykanymi na dwa zamki, oraz dodatkowo wewnętrznymi drzwiami antywłamaniowymi zamykanymi na jeden zamek.
   2) bocznym, od frontu po lewej stronie (wejście do ajencji Banku PKO BP) zabezpieczone drzwiami z dwoma zamkami i dodatkowo wewnętrzną kratą drzwiową.
2. Poszczególne pokoje, w których odbywa się przetwarzanie danych osobowych i ich składowanie muszą być wyposażone w co najmniej jeden zamek i muszą być zamykane podczas nieobecności pracownika. Po zakończeniu pracy osoba zamykająca pomieszczenie powinna przekazać klucz sprzątaczce, bądź umieścić go w specjalnie przeznaczonej gablocie.
3. Stanowiska komputerowe w pomieszczeniach gdzie mogą przebywać osoby nieuprawnione do przetwarzania danych osobowych (np. interesanci albo inni pracownicy Urzędu) winny być umieszczone w sposób, który uniemożliwi takim osobom wgląd do tych danych. W pokoju, do którego dostęp maja petenci monitory komputerowe winny być ustawione w ten sposób, by petenci nie widzieli zapisów na ekranie.
4. W przypadku dłuższej bezczynności uruchamiane są tzw. wygaszacze ekranu.
5. Wydruki zawierające dane osobowe powinny znajdować się w miejscu, które uniemożliwia dostęp osobom postronnym.
6. Kopie bezpieczeństwa (kopie zapasowe) wykonują okresowo pracownicy w ramach swoich obowiązków. Kopie bezpieczeństwa przechowywane są w szafie metalowej w pok. Nr 4 i w pok. Nr 7 Urzędu. Dostęp do nośników zawierających kopie danych maja tylko uprawnione osoby.
7. Wydruk z ważnym hasłem należy przechowywać tak by uniemożliwić dostęp do niego osobom postronnym (innym niż użytkownik, przełożeni i Administrator).

Rozdział V. Zabezpieczenia niefizyczne

§ 9

1. Zalogowanie się do systemu wymaga podania nazwy użytkownika i hasła. Każdy użytkownik ma przypisane uprawnienia do wykonania operacji. Nieudane próby logowania są rejestrowane, a po 3 nieudanych próbach logowania następuje czasowa blokada konta użytkownika na stacji roboczej.
2. Dostęp do stacji roboczych chroniony jest hasłem.
3. Oprogramowanie wykorzystywane do przetwarzania danych posiada własny (dodatkowy, oprócz systemowego) system autoryzacji użytkownika.
4. Wykorzystywany jest system szyfrowania danych (dostępny w systemie operacyjnym) uniemożliwiający odczyt danych osobowych osobom nieupoważnionym.

5. W celu ochrony przed dostępem do danych komputera z sieci publicznej wykorzystuje się programową zaporę ogniową (ang. firewall) zarówno w przypadku stacji roboczych jak i serwerów.
6. Zgodnie z przyjętym harmonogramem wykonuje się kopie bezpieczeństwa (kopie zapasowe).

Rozdział VI. Monitorowanie zabezpieczeń

§ 10

1. Do monitorowania systemu zabezpieczeń, stosownie do swojego zakresu czynności zobligowani są:
   1) Administrator danych,
   2) Administrator bezpieczeństwa informacji,
   3) Administrator systemu informatycznego.
2. W ramach monitoringu należy przeprowadzić następujące działania:
   1) okresowe sprawdzanie kopi bezpieczeństwa pod względem przydatności do odtworzenia danych,
   2) sprawdzania częstotliwości zmian haseł.
3. Administrator bezpieczeństwa informacji sporządza roczny plan kontroli, który podlega zatwierdzeniu przez Administratora danych i zgodnie z nim przeprowadza kontrole oraz dokonuje oceny stanu bezpieczeństwa danych osobowych.
4. Na podstawie zgromadzonych informacji sporządza roczne sprawozdanie i przedstawia je Administratorowi danych.

Rozdział VII. Obowiązki Administratora danych

§ 11

1. Do obowiązków Administratora danych należy w szczególności:
   1) zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym,
   2) zapobieganie zabraniu danych przez osobę nieuprawnioną,
   3) zapobieganiu przetwarzaniu danych z naruszeniem przepisów prawa ich zmianie, utracie, uszkodzeniu lub zniszczeniu,
   4) zbierania danych dla oznaczonych, zgodnych z prawem celów,
   5) dbałość o merytoryczną poprawność danych i adekwatność w stosunku do celów w jakich są przetwarzane,
   6) opracowanie instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych, przeznaczoną dla osób zatrudnionych przy przetwarzaniu tych danych,
   7) określenie budynków, pomieszczeń lub części pomieszczeń, tworzące obszar w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego,
   8) opracowanie instrukcji, określającej sposób zarządzania systemem informatycznym. Służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji,
   9) prowadzenie ewidencji osób uprawnionych do przetwarzania dany osobowych,
   10) organizowanie szkoleń mających na celu zaznajomienie każdej osoby przetwarzającej dane osobowe z przepisami dotyczącymi ich ochrony.

2. Administrator danych odpowiada za to by zakres czynności osoby zatrudnionej przy przetwarzaniu danych osobowych określał odpowiedzialność tej osoby za:
   1) ochronę danych przed niepowołanym dostępem,
   2) nieuzasadnioną modyfikację lub zniszczenie danych,
   3) nielegalne ujawnienie danych.

   w stopniu odpowiednim do zadań realizowanych w procesie przetwarzania danych osobowych.

Rozdział VIII. Obowiązki Administratora bezpieczeństwa informacji

§ 12

Do obowiązków Administratora bezpieczeństwa informacji należy w szczególności:
1) nadzór nad przestrzeganiem instrukcji określającej sposób zarządzania systemem informatycznym,
2) przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe,
3) podejmowanie odpowiednich działań w celu właściwego zabezpieczenia danych osobowych,
4) badanie ewentualnych naruszeń w systemie zabezpieczeń danych osobowych,
5) podejmowanie decyzji o instalowaniu nowych urządzeń oraz oprogramowania wykorzystywanego do przetwarzania danych osobowych,
6) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych zawierających dane osobowe,
7) nadzór nad wykonywaniem kopii zapasowych i ich przechowywaniem,
8) wdrożenie szkoleń z zakresu przepisów dotyczących ochrony danych osobowych, środków technicznych i organizacyjnych stosowanych przy przetwarzaniu danych w systemach informatycznych,
9) sporządzanie planów kontroli zatwierdzanych przez Administratora danych i przeprowadzanie zgodnie z planem kontroli,
10) sporządzanie raportów z naruszenia bezpieczeństwa systemu informatycznego.

Rozdział VIX. Obowiązki Administratora systemu informatycznego

§ 13

Do obowiązków Administratora systemu informatycznego należy w szczególności:
1) naprawa, konserwacja oraz likwidacja urządzeń komputerowych zawierających dane osobowe,
2) definiowanie użytkowników i haseł dostępu w systemie,
3) aktualizowanie oprogramowania systemowego, chyba że aktualizacje wykonywane są automatycznie,
4) aktualizowanie oprogramowania antywirusowego, chyba że aktualizacje wykonywane są automatycznie,
5) okresowe sprawdzanie kopii zapasowych pod kątem ich dalszej przydatności,

Rozdział X. Postępowanie w przypadku naruszenia ochrony danych osobowych

§ 14

1. Każdy pracownik Urzędu, który poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe, bądź posiada informację, mogącą mieć wpływ na bezpieczeństwo danych osobowych, jest zobowiązany fakt ten natychmiast zgłosić Administratorowi bezpieczeństwa informacji.
2. W razie niemożności zawiadomienia Administratora bezpieczeństwa informacji, należy powiadomić bezpośredniego przełożonego.
3. W przypadku wykrycia naruszenia ochrony danych osobowych Administrator bezpieczeństwa informacji informuje Wójta i Sekretarza Gminy o zaistniałym zdarzeniu oraz przeprowadza dochodzenie, po czym sporządza raport opisując okoliczności zdarzenia, którego wzór stanowi załącznik nr 4 do Polityki. Jeśli zdarzenie ma charakter przestępstwa sprawa kierowana jest do organów ścigania.

Załącznik nr 1
do Polityki bezpieczeństwa
Urzędu Gminy w Dąbrównie

Dąbrówno, dn. .....

.....
(imię i nazwisko pracownika)

.....
(adres)

Oświadczenie

1. Stwierdzam własnoręcznym podpisem, że znana jest mi treść przepisów:
   1) o ochronie i postępowaniu z wiadomościami stanowiącymi tajemnicę służbową,
   2) o zasadach ochrony oraz środkach i zabezpieczeniach danych osobowych (Dz. U. nr 133, poz. 833) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 28 kwietnia 2004 r. (Dz. U. nr 1090, poz. 1024) oraz o odpowiedzialności karnej za naruszenie ochrony danych osobowych.

2. Jednocześnie zobowiązuję się nie ujawniać wiadomości, z którymi zapoznałem/zapoznałam* się z racji wykonywanej pracy w Urzędzie Gminy w Dąbrównie, a w szczególności nie będę:
   1) ujawniać danych zawartych w eksploatowanych w Urzędzie systemach informatycznych, zwłaszcza danych osobowych znajdujących się w tych systemach,
   2) ujawniać szczegółów technicznych używanych w Urzędzie systemów oraz oprogramowania,
   3) udostępniać osobom nieupoważnionym nośniki magnetyczne i optyczne oraz wydruki komputerowe,
   4) kopiować lub przetwarzać danych w sposób inny niż dopuszczony obowiązującą instrukcją technologiczną.

.....
(podpis pracownika)

.....
(podpis przełożonego)

* niepotrzebne skreślić

Załącznik nr 2
do Polityki bezpieczeństwa
Urzędu Gminy w Dąbrównie

Wykaz osób, które zostały zapoznane z „Polityką bezpieczeństwa Urzędu Gminy w Dąbrównie"

Lp.	Nazwisko i imię	Stanowisko	Podpis pracownika

Załącznik nr 3
do Polityki bezpieczeństwa
Urzędu Gminy w Dąbrównie

Wykaz zbiorów danych osobowych
znajdujących się w Urzędzie Gminy Dąbrówno

Lp.	Zbiór danych	Forma przetwarzania	Nazwa oprogramowania (producent)	Nr pokoju
1.	1) Kadry	1) ręcznie i komputerowo	1) KADRY – system SOJST PUMA (Zakład Elektronicznej Techniki Obliczeniowej Sp. z.o.o. w Olsztynie)	1
	2) Sprawozdania Systemu Informacji	2) komputerowo	2) System Informacji Oświatowej	
	3) Baza płatników składek ZUS (pracowników)	3) komputerowo	3) PŁATNIK (PROKOM Asseco Poland S.A. w Rzeszowie	
2.	Rejestr decyzji o warunkach zabudowy i zagospodarowania terenu	ręcznie	xxx	2
3.	1) Windykacja podatków i opłat lokalnych	1) komputerowo	1) OPŁATY – system SOJST PUMA (Zakład Elektronicznej Techniki Obliczeniowej Sp. z.o.o. w Olsztynie)	3
	2) Ewidencja podatników podatku i opłat lokalnych	2) komputerowo	2) GRUNTY- podatek od osób fizycznych; OPJ – podatek od osób prawnych; POJAZDY- podatek od środków transportowych: system SOJST PUMA (Zakład Elektronicznej Techniki Obliczeniowej Sp. z.o.o. w Olsztynie)	

4.	Baza właścicieli nieruchomości	komputerowo	EWOPIS WIN i EWMAPA VIEW (Firma GEOOBID Sp. z.o.o. w Katowicach)	6
5.	1) Ewidencja Ludności oraz danych w dowodach osobistych	1) Ręcznie i komputerowo	1) EWIDENCJA LUDNOŚCI – system SOJST PUMA (Zakład Elektronicznej Techniki Obliczeniowej Sp. z.o.o. w Olsztynie) System Wydawania Dowodów Osobistych (WASKO S.A. w Gliwicach)	7
	2) Urząd Stanu Cywilnego	2) Ręcznie i komputerowo	2) URZĄD STANU CYWILNEGO – system SOJST PUMA (Zakład Elektronicznej Techniki Obliczeniowej Sp. z.o.o. w Olsztynie)	
	3) Rejestr działalności Gospodarczych	3) Ręcznie i komputerowo	3) EWIDENCJA PODMIOTÓW GOSPODARCZYCH – system SOJST PUMA (Zakład Elektronicznej Techniki Obliczeniowej Sp. z.o.o. w Olsztynie)	
	4) Rejestr wydanych decyzji na sprzedaż napojów alkoholowych	4) Ręcznie i komputerowo	4) KONCESJE ALKOHOLOWE – system SOJST PUMA (Zakład Elektronicznej Techniki Obliczeniowej Sp. z.o.o. w Olsztynie)	

Załącznik nr 4
do Polityki bezpieczeństwa
Urzędu Gminy w Dąbrównie

Raport z naruszenia bezpieczeństwa systemu informatycznego w Urzędzie Gminy Dąbrówno

1. Data: ..... Godzina: .....
(dd.mm.rr.) (gg.mm.)

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....
(imię, nazwisko, stanowisko, nazwa użytkownika (jeśli występuje))

3. Lokalizacja zdarzenia:

.....
(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....
.....
.....

5. Przyczyny wystąpienia zdarzenia:

.....
.....
.....

6. Podjęte działania:

.....
.....
.....

7. Postępowanie wyjaśniające:

.....
.....
.....

.....
(data, podpis Administratora bezpieczeństwa informacji)

Załącznik Nr 2
do Zarządzenia Nr Or. 0153-196/10
Wójta Gminy Dąbrówno
z dnia 23 lutego 2010 r.

Instrukcja zarządzania systemem informatycznym
Służącym do przetwarzania danych osobowych
w Urzędzie Gminy Dąbrówno

I. Postanowienia ogólne

§ 1

Niniejszy dokument został opracowany na podstawie § 3 i 5 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).

§ 2

1. Ilekroć mowa w niniejszym dokumencie o Instrukcji, należy przez to rozumieć „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Dąbrówno".
2. Ilekroć mowa w niniejszym dokumencie o Urzędzie, należy przez to rozumieć Urząd Gminy Dąbrówno.

II. Zagadnienia organizacyjne

§ 3

1. Pracownicy upoważnieni do przetwarzania danych osobowych w systemie informatycznym, jak i ręcznym, zobowiązani są do zapoznania się z treścią Instrukcji i jej bezwzględnego przestrzegania.
2. Fakt zapoznania się z Instrukcją, pracownik potwierdza własnoręcznym podpisem na stosownym wykazie, którego wzór stanowi załącznik nr 1 do Instrukcji.

III. Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie

§ 4.

1. Przed rozpoczęciem pracy z systemem informatycznym oraz w trakcie pracy każdy pracownik obowiązany jest do zwrócenia bacznej uwagi, czy nie wystąpiły symptomy mogące świadczyć o naruszeniu ochrony danych osobowych. W przypadku ich wykrycia, należy niezwłocznie powiadomić o tym fakcie Administratora bezpieczeństwa informacji.
2. W celu rozpoczęcia pracy użytkownik wykonuje logowanie do systemu używając nadanego loginu i hasła.
3. Podczas nieobecności przy stanowisku komputerowym, należy wylogować się z systemu, bądź uruchomić wygaszasz ekranu.
4. Po zakończeniu pracy w systemie, należy wylogować się z systemu i wyłączyć stację roboczą.

5. Zawieszenie korzystania z systemu informatycznego może nastąpić losowo wskutek awarii lub planowo (np. w celu konserwacji sprzętu). Planowe zawieszenie prac jest uprzedzone informacją do pracowników Urzędu (w formie wiadomości e-mail lub osobiście) przez Administratora systemu na co najmniej 30 minut przed planowanym zawieszeniem.

IV. Nadawanie uprawnień

§ 5

1. Przetwarzać dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych, którego wzór stanowi załącznik Nr 2 do Instrukcji.
2. Uprawnienia do przetwarzania danych osobowych w systemie informatycznym Urzędu nadaje Administrator danych.

V. Zabezpieczenia

§ 6

1. Ochronę przed awariami zasilania oraz zakłóceniami w sieci energetycznej serwera i stacji roboczych, na których przetwarzane są dane osobowe zapewniają zasilacze UPS.
2. Hasła do systemu stacji roboczych kontrolowanych przez domeny (PDC) mają długość co najmniej 8 znaków, w tym co najmniej, 1 cyfra i 1 duża litera i okres ważności hasła ustawiony na okres nie dłuższy niż 30 dni.
3. Oprogramowanie wykorzystane do przetwarzania danych posiada własny system kont (zabezpieczonych hasłami) i uprawnieniami. Za okresową (przynajmniej co 30 dni) zmianę hasła odpowiada użytkownik oprogramowania.
4. Stosuje się aktywną ochronę antywirusową lub w przypadku braku takiej możliwości przynajmniej raz w tygodniu skanowanie całego systemu (w poszukiwaniu „złośliwego oprogramowania") na każdym komputerze, na którym przetwarzane są dane osobowe. Za dokonywanie skanowania systemu w poszukiwaniu „złośliwego oprogramowania" (w przypadku braku ochrony rezydentnej) i aktualizację bazy wirusów odpowiada użytkownik stacji roboczej.

VI. Procedury tworzenia kopii zapasowych

§ 7

1. Dane systemów kopiowane są w trybie tygodniowym (pn.-pt. kopie baz danych; pn.-pt. kopia awaryjna - kopia bezpieczeństwa systemu serwera). Kopie awaryjne danych zapisanych w programach wykonywane są codziennie, po zakończeniu pracy. Odpowiedzialnym za wykonanie kopii danych jest pracownik obsługujący dany program przetwarzający dane. Kopie zbiorów umieszczone na serwerze wykonywane są automatycznie dedykowanym oprogramowaniem.
2. Kopie awaryjne są przechowywane w szafie metalowej w pokoju Nr 7 Urzędu. Osoba odpowiedzialną za wykonanie kopii awaryjnych jest Administrator systemu.
3. Okresową weryfikację kopii awaryjnych (bezpieczeństwa) pod kontem ich przydatności do odtwarzania danych przeprowadza Administrator systemu.
4. Nośniki danych, na których zapisane są kopie awaryjne (bezpieczeństwa) niszczy się trwale w sposób mechaniczny.

VII. Odnotowywanie udostępniania danych

§ 8

1. System informatyczny przetwarzający dane musi posiadać mechanizmy pozwalające na odnotowanie faktu wykonania operacji na danych. W szczególności zapis ten powinien obejmować:
   1) rozpoczęcie i zakończenie pracy przez użytkownika systemu,
   2) operacje wykonywane na przetwarzanych danych,
   3) przesyłanie za pośrednictwem systemu danych osobowych przetwarzanych w systemie informatycznym innym podmiotom nie będącym właścicielem ani współwłaścicielem systemu,
   4) nieudane próby dostępu do systemu informatycznego przetwarzającego dane osobowe oraz nieudane próby wykonania operacji na danych osobowych,
   5) błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.
2. System informatyczny powinien zapewnić zapis faktu przekazania danych osobowych z uwzględnieniem:
   1) identyfikatora osoby, której dane dotyczą,
   2) osoby przesyłającej dane,
   3) odbiorcy danych,
   4) zakresu przekazanych danych osobowych,
   5) daty operacji,
   6) sposobu przekazania danych.

VIII. Procedury wykonywania przeglądów i konserwacji systemów

§ 9

1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe mogą być wykonywane wyłącznie przez pracowników Urzędu lub przez upoważnionych przedstawicieli wykonawców.
2. Prace , o których mowa w ust 1 powinny uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.
3. Przed rozpoczęciem prac, o których mowa w ust. 1 przez osoby niebędące pracownikami Urzędu, należy dokonać potwierdzenia tożsamości tychże osób.

IX. Niszczenie wydruków i nośników danych

§ 10

1. Nośniki magnetyczne przekazywane na zewnątrz powinny być pozbawione zapisów zawierających dane osobowe. Niszczenie poprzednich zapisów powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika.
2. Poprawność przygotowania nośnika magnetycznego powinna być sprawdzona praz Administratora bezpieczeństwa informacji.
3. Uszkodzenie nośniki magnetycznego przed ich wyrzuceniem należy fizycznie zniszczyć (przeciąć, przełamać , itp.).
4. Po wykorzystaniu wydruki zawierające dane osobowe powinny być niszczone w niszczarce.

Załącznik Nr 1
do Instrukcji zarządzania systemem informatycznym
służącym do przetwarzania danych osobowych
w Urzędzie Gminy Dąbrówno

Upoważnienie
(wzór)

Na podstawie 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.) Administrator danych Urzędu Gminy Dąbrówno **u p o w a ż n i a** Pana/Panią*:

.....
(Imię, nazwisko, stanowisko)

do przetwarzania danych osobowych w zbiorach:

.....
(Nazwa zbioru)

Administrator danych zobowiązuje Pana/Panią* do przestrzegania wyżej cytowanej ustawy i wydanych na jej podstawie Rozporządzeń oraz do przestrzegania „Polityki bezpieczeństwa Urzędu Gminy Dąbrówno i Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Dąbrówno".

Pouczenie:
Osoba upoważniona obowiązana jest do zachowania w tajemnicy informacje uzyskane w trakcie dokonywania operacji związanych z gromadzeniem i przetwarzaniem danych osobowych. Obowiązek ten istnieje w trakcie zatrudnienia, jak również po ustaniu (rozwiązaniu) zatrudnienia.

Przyjąłem/Przyjęłam* do wiadomości i stosowania

.....
(Data i podpis upoważnionego pracownika)

.....
(Podpis Administratora danych osobowych w Urzędzie Gminy Dąbrównie)

* niepotrzebne skreślić

Załącznik Nr 2
do Instrukcji zarządzania systemem informatycznym
służącym do przetwarzania danych osobowych
w Urzędzie Gminy Dąbrówno

Wykaz osób, które zostały zapoznane z „Instrukcją zarządzania systemem informatycznym służącym do przetwarza danych osobowych w Urzędzie" Gminy Dąbrówno"

L.p.	Imię i nazwisko	Stanowisko	Data	Podpis