Zarządzenie Nr 176A/09
Wójta Gminy Pątnów
z dnia 05 maja 2009r.

w sprawie: wprowadzenia dokumentacji opisującej sposób przetwarzania danych osobowych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych.

Na podstawie art 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz § 3 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 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) :

zarządzam co następuje

§ 1. Wprowadzam dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych w Urzędzie Gminy w Pątnowie.

§ 2. Na dokumentację składa się:
1) Polityka bezpieczeństwa zarządzania systemem informatycznym służącym do przetwarzania danych osobowych stanowiąca załącznik nr 1 do zarządzenia,
2) Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych Urzędzie Gminy w Pątnowie stanowiąca załącznik nr 2 do zarządzenia,
3) Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych stanowiąca załącznik nr 3 do zarządzenia.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

Wójt
mgr Grzegorz Smudowski

Załącznik Nr 1
do Zarządzenia Nr 176A/2009
Wójta Gminy Pątnowie
z dnia 5.05. 2009 r.

Polityka bezpieczeństwa danych osobowych.

ROZDZIAŁ I.

Postanowienia ogólne.

§1. Polityka bezpieczeństwa reguluje sposób zarządzania, ochrony i dystrybucji danych osobowych w Urzędzie Gminy w Pątnowie.

§2. Celem polityki bezpieczeństwa jest określenie środków technicznych i organizacyjnych oraz ustanowienie zasad i reguł postępowania w zakresie zabezpieczenia danych osobowych.

§3. Ilekroć w polityce bezpieczeństwa jest mowa o:
- urzędzie – rozumie się przez to Urząd Gminy w Pątnowie,
- obszarze przetwarzania danych osobowych – rozumie się przez to wydzieloną część budynku Urzędu, w której przetwarzane są dane osobowe,
- poufności danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nie upoważnionym podmiotom,
- integralności danych – rozumie się przez to właściwość zapewniając że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
- rozliczalność – rozumie się przez to właściwość że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
- identyfikatorze – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
- haśle – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
- ustawie – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Z 2002 r. Nr 101, poz. 926 z późn. zm.).

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

§ 4.1. Dane osobowe przetwarzane są w budynku Urzędu położonym w miejscowości Pątnów 48. Wszystkie zarejestrowane i wymienione niżej zbiory przetwarzane są tylko i wyłącznie w w/w budynku Urzędu.
2. Obszarem, w którym przetwarzane są dane osobowe – są następujące pomieszczenia biurowe:

1) parter – pokój nr 3,
2) I piętro – pokój nr 6,
3) I piętro – pokój nr 7,
4) I piętro – pokój nr 10,
5) I piętro – pokój nr 16
6) I piętro – pokój nr 17
7) I piętro – pokój nr 4
8) I piętro – pokój nr 11

ROZDZIAŁ III.
Wykaz zbiorów danych osobowych oraz programów do ich przetwarzania.

§ 5. W urzędzie prowadzi się następujące zbiory danych osobowych w następujących obszarach.

L.p.	*Nazwa zbioru danych*	*Forma przetwarzania zbioru*	*Pokój*
1.	Rejestr wydanych decyzji o warunkach zabudowy i zagospodarowania terenu	papierowa	17
2.	Ewidencja skarg i wniosków	papierowa	4
3.	Decyzje pozwoleń na budowę	papierowa	17
4.	Plan urządzenia lasów nie stanowiących własności skarbu państwa	papierowa	11
5.	Dzierżawa gruntów i opłaty za użytkowanie wieczyste	papierowa	11
6.	Rejestr przedpoborowych i poborowych	papierowa	3
7.	Rejestr formacji obrony cywilnej	papierowa	3
8.	Ewidencja ludności i dowody osobiste	komputerowa	3
9.	Zobowiązania pieniężne ludności	komputerowa	7
10.	Podatki i opłaty lokalne	komputerowa	7
11.	Kopie aktów własności ziemi	papierowa	11
12.	Oświadczenia o stanie majątkowym radnych	papierowa	4
13.	Zbiór aktów notarialnych dotyczących zbycia nieruchomości	papierowa	7
14.	Skład komitetu przeciwpowodziowego wraz z drużynami ratowniczymi	papierowa	3
15	Stypendia	papierowa	16

§ 6. Zbiory w systemach informatycznych przetwarzane są przy zastosowaniu następujących programów i w następujących obszarach:

1. Pozycja 8 powyższej tabeli:
   1) Zbiór danych osobowych przetwarzany jest za pomocą programu SELWIN,
   2) Zbiór danych wraz z oprogramowaniem zamontowane są na stacji roboczej znajdującej się w pokoju Nr 3.
2. Pozycja 8 powyższej tabeli:
   1) Zbiór danych osobowych przetwarzany jest za pomocą programu SWDO.

2) Zbiór danych wraz z oprogramowaniem zamontowane są na stacji roboczej znajdującej się w pokoju Nr 3.

3. Pozycja 10 powyższej tabeli:
   1) Zbiór danych osobowych przetwarzany jest za pomocą modułów programu Podatki, Księgowość Zobowiązań.
   2) Oprogramowanie zamontowane jest na stacjach roboczych znajdujących się w pokoju Nr 7.
   3) Baza danych zamontowana jest na bazodanowym serwerze znajdującym się w pokoju Nr 8

ROZDZIAŁ IV.
Opis struktury zbiorów danych osobowych.

1. W zbiorze danych „Rejestr wydanych decyzji o warunkach zabudowy i zagospodarowania terenu" – l.p. 1 w tabeli – przetwarzane są dane osobowe w zakresie:
a) nazwiska i imiona
b) adres zamieszkania lub pobytu

2. W zbiorze danych „Ewidencja skarg i wniosków" – l.p. 2 w tabeli przetwarzane są dane osobowe w zakresie:
a) nazwiska i imiona
b) adres zamieszania lub pobytu

3. W zbiorze danych „Decyzje pozwoleń na budowę" – l.p. 3 w tabeli – przetwarzane są dane osobowe w zakresie:
a) nazwiska i imiona
b) adres zamieszkania lub pobytu
c) numer działki

4. W zbiorze danych „Plan urządzenia lasów nie stanowiących własności skarbu państwa" – l.pl 4 w tabeli przetwarzane są dane osobowe w zakresie:
a) nazwiska i imiona
b) adres zamieszkania lub pobytu
c) numer działki

5.W zbiorze danych „Dzierżawa gruntów i opłaty za użytkowanie wieczyste" – l.p. 5 w tabeli – przetwarzane są dane osobowe w zakresie:
a) nazwiska i imiona
b) imiona rodziców
c) adres zamieszkania lub pobytu
d) seria i numer dowodu osobistego
e) numer, powierzchnia i obręb geodezyjny działki
f) klasa gruntów

g) wysokość opłat

6. W zbiorze danych „Rejestr przedpoborowych i poborowych" – l.p. 6 w tabeli – przetwarzane są dane osobowe w zakresie:
a) nazwiska i imiona
b) imiona rodziców
c) data urodzenia
d) adres zamieszkania lub pobytu
e) numer ewidencyjny PESEL
f) wykształcenie
g) seria i numer dowodu osobistego
h) kategoria zdrowia
i) numer książeczki wojskowej

7. W zbiorze danych „Rejestr formacji obrony cywilnej" – l.p. 7 w tabeli – przetwarzane są dane osobowe w zakresie:
a) nazwiska i imiona
b) imiona rodziców
c) data urodzenia
d) adres zamieszkania lub pobytu
e) miejsce pracy
f) seria i numer dowodu osobistego
g) stopień wojskowy
h) pełniona funkcja
i) numer karty przydziału

8. W zbiorze danych „Ewidencja ludności i dowody osobiste" – l.p. 8 w tabeli – przetwarzane są dane osobowe w zakresie:
a) nazwiska i imiona
b) imiona rodziców
c) data urodzenia
d) adres zamieszkania lub pobytu
e) numer ewidencyjny PESEL
f) miejsce pracy
g) zawód
h) wykształcenie
i) seria i numer dowodu osobistego

9. W zbiorze danych „Zobowiązania pieniężne ludności" – l.p. 9 w tabeli – przetwarzane są dane osobowe w zakresie:
a) nazwiska i imiona
b) adres zamieszkania lub pobytu
c) imiona rodziców

10. W zbiorze danych „Podatki i opłaty lokalne" – l.p. 10 w tabeli – przetwarzane są dane osobowe w zakresie:
a) nazwiska i imiona
b) imiona rodziców
c) adres zamieszkania lub pobytu

11. W zbiorze danych „Kopie aktów własności ziemi" – l.p. 11 w tabeli przetwarzane są dane osobowe w zakresie:
a) nazwiska i imiona
b) imiona rodziców
c) data urodzenia
d) adres zamieszkania lub pobytu
e) numer, powierzchnia i obręb geodezyjny działki

12. W zbiorze danych „Oświadczenia o stanie majątkowym radnych" – l.p. 12 w tabeli – przetwarzane są dane osobowe w zakresie:
a) nazwiska i imiona
b)data urodzenia
c)adres zamieszkania lub pobytu

13. W zbiorze danych „Zbiór aktów notarialnych dotyczących zbycia nieruchomości" – l.p. 13 w tabeli – przetwarzane są dane osobowe w zakresie:
a) nazwiska i imiona
b) imiona rodziców
c) adres zamieszkania lub pobytu
d) seria i numer dowodu osobistego
e) numer, powierzchnia i obręb geodezyjny działki
f) numer księgi wieczystej

14. W zbiorze danych „Skład komitetu przeciwpowodziowego wraz z drużynami ratowniczymi" – l.p. 14 w tabeli – przetwarzane są dane osobowe w zakresie:
a) nazwiska i imiona
b) adres zamieszkania lub pobytu
c) miejsce pracy

15. W zbiorze danych „Stypendia" – l.p. 16 w tabeli – przetwarzane są dane osobowe w zakresie:
a) nazwiska i imiona
b) imiona rodziców
c) data urodzenia
d) miejsce pracy
e) wynagrodzenie

ROZDZIAŁ V.
Sposób przepływu danych pomiędzy systemami.

§ 8. Przepływ danych pomiędzy systemami informatycznymi występuje w Urzędzie w następujących zbiorach:

1. SWDO – SELWIN.
   Przepływ danych z systemu przetwarzającego zbiór danych osobowych "SWDO" do sytemu przetwarzającego zbiór danych osobowych "SELWIN" polega na

wprowadzeniu przez upoważnionego do obsługi tych systemów pracownika, serii i numeru dowodu osobistego nadanego przez system przetwarzający zbiór danych "Dowody osobiste".

2. Dowody osobiste - Ministerstwo Spraw Wewnętrznych i Administracji.
   Przepływ danych wymuszony ustawowo za pomocą teletransmisji polega na pobieraniu danych ze zbioru p.n. Dowody osobiste do zbioru, którego administratorem jest MSWiA.
3. SELWIN
   Przepływ polega na przesyłaniu jeden raz w tygodniu kopii bazy danych zapisanych na zewnętrznym nośniku informacji – (dyskietka) – oraz wszystkich składowych systemu informatycznego w formie papierowej do T.B.D. Oddziału w Sieradzu Wysłane materiały są zwracane drogą pocztową do urzędu po aktualizacji zbioru w T.B.D.
4. Podatki – Księgowość zobowiązań.
   Są to dwa systemy informatyczne wykorzystujące jedną bazę danych osobowych. System Księgowość zobowiązań jedynie współdzieli bazę danych osobowych z systemem Podatki . Przepływ danych pomiędzy tymi systemami odbywa się na drodze programowej.

ROZDZIAŁ VI.

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

§ 9. Mając na uwadze fakt, iż w systemach informatycznych nie są przetwarzane dane wrażliwe – wprowadza się w Urzędzie **podstawowy poziom bezpieczeństwa** przetwarzania danych osobowych w systemach informatycznych.

§ 10. W celu zapewnienia poufności przetwarzanych danych stosuje się w Urzędzie następujące środki:

1) udostępnianie danych ze zbioru danych osobowych odbywa się wyłącznie na pisemny wniosek z podaniem ich wykorzystania,
2) urządzenia systemu informatycznego (monitory, drukarki itp.) sytuuje się w sposób uniemożliwiający osobom postronnym wgląd w przetwarzane dane.

§ 11. W celu zapewnienia integralności danych stosuje się w Urzędzie szereg zabezpieczeń obszarów przetwarzania danych oraz urządzeń wchodzących w skład systemów informatycznych. Obszary i urządzania do przetwarzania danych osobowych zabezpiecza się przed:

1. Zagrożeniami losowymi zewnętrznymi (klęski żywiołowe, przerwy w zasilaniu, wyładowania atmosferyczne, awarie urządzeń, itp.) poprzez :
   1) stosowanie elementów filtrujących i podtrzymujących napięcie na elementach zasilających,
   2) odpowiednie zabezpieczenie przeciwpożarowe,
   3) umiejscowienie elementów systemu informatycznego w odległości bezpiecznej od okien, kaloryferów i innych urządzeń, których awaria mogłaby zagrozić integralności baz danych,
   4) zabezpieczenie drzwi dwoma zamkami patentowymi, zabezpieczenie okien stalową kratą na parterze.

2. Zagrożeniami losowymi wewnętrznymi (niezamierzone pomyłki operatorów, awarie sprzętowe, błędy oprogramowania itp.) poprzez:
    1) stworzenie odpowiednich warunków do pracy,
    2) stosowanie markowych urządzeń nie powodujących wzajemnych konfliktów,
    3) tworzenie i przechowywanie kopii baz danych,
    4) szkolenia i ciągłe podnoszenie świadomości operatorów systemów informatycznych.
3. Zagrożeniami zamierzonymi (nieuprawniony dostęp do systemu z zewnątrz, nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych itp.) poprzez:
    1) odpowiednie zabezpieczenie wszystkich dróg dojścia do obszaru przetwarzania danych osobowych (drzwi – podwójne zamki patentowe, okna – stalowa krata),
    2) stosowanie mechanizmów uwierzytelniania operatora (identyfikator, hasło),
    3) odnotowywanie przez oprogramowanie służące do przetwarzania danych osobowych ważniejszych działań operatorów w systemie,
    4) całkowity zakaz instalowania na stanowiskach komputerowych, na których przetwarzane są dane osobowe oprogramowania innego niż przydzielone przez Administratora Bezpieczeństwa Informacji,
    5) ustalenie zasad archiwizacji,
    6) całkowity zakaz przebywania osób nieuprawnionych w obszarze przetwarzania danych osobowych, w przypadku nieobecności w nim osoby upoważnionej do przetwarzania tych danych,
    7) serwisowanie lub naprawę elementów systemu informatycznego przez pracowników z zewnątrz - jedynie w obecności operatora systemu informatycznego lub innej osoby upoważnionej przez administratora danych.

Załącznik Nr 2
do Zarządzenia Nr 176A/2009
Wójta Gminy Pątnów
z dnia 05 maja 2009 r.

INSTRUKCJA
zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.

ROZDZIAŁ I.
Postanowienia ogólne.

§ 1. Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych zwana w dalszej treści "Instrukcją" określa podstawowe środki ochrony danych i elementy zarządzania systemem informatycznym.

§ 2. Instrukcja przeznaczona jest dla osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych w Urzędzie Gminy w Pątnowie zwanym w dalszej treści "Urzędem".

§ 3. Ilekroć w instrukcji jest mowa o:

a) ustawie – należy przez to rozumieć ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.),

b) rozporządzeniu – należy przez to rozumieć 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. Nr 100, poz. 1024).

ROZDZIAŁ II.
Procedury nadawania uprawnień do przetwarzania danych.

§ 4. Stanowiska pracy w Urzędzie mogą prowadzić tylko takie zbiory danych osobowych, na które pozwalają przepisy prawne w randze ustawy, a zbiór został zgłoszony do Generalnego Inspektora Ochrony Danych Osobowych celem rejestracji.

§ 5. Do obsługi systemu informatycznego służącego do przetwarzania danych osobowych dopuszczeni są wyłącznie pracownicy Urzędu posiadający pisemne upoważnienie wydane przez Wójta Gminy.

1) warunkiem wydania upoważnienia jest przeszkolenie pracownika w zakresie ochrony danych osobowych przez Administratora Bezpieczeństwa Informacji.

2) fakt zapoznania z obowiązującymi przepisami – pracownik potwierdza pisemnie złożonym oświadczeniem.

§ 6. Osobą odpowiedzialną za nadawanie uprawnień do przetwarzania danych w systemie informatycznym jest administrator danych - Wójt Gminy.

a) W celu nadania, zmiany lub odebrania uprawnień do przetwarzania danych osobowych, administrator danych udziela upoważnienia bądź zawiadamia o utracie

przez daną osobę uprawnień do przetwarzania danych osobowych w systemie informatycznym.

§ 7. 1.Po otrzymaniu upoważnienia do przetwarzania danych – pracownik składa pisemne oświadczenie o zachowaniu w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia.

§ 8. 1. Osobą odpowiedzialną za rejestrowanie uprawnień w systemie informatycznym jest Administrator Bezpieczeństwa Informacji zwany w dalszej treści Instrukcji "ABI".

2. Procedura rejestrowania uprawnień w systemie informatycznym (upoważnienie) jest następująca:

1) ABI ustala identyfikator użytkownika i wraz z zakresem uprawnień, odnotowuje ten fakt w prowadzonej ewidencji osób upoważnionych do przetwarzania danych osobowych w Urzędzie,
2) ABI przydziela pierwsze hasło dla osoby upoważnionej,
3) osoba upoważniona potwierdza własnoręcznym podpisem przydział identyfikatora i pierwszego hasła, które jest zobowiązana zmienić przy następnym logowaniu się do systemu,
4) ABI tworzy w systemie informatycznym profil użytkownika.

3. Procedura zmiany lub odebrania uprawnień do przetwarzania danych osobowych (zawiadomienie) – jest następująca:

1) ABI odnotowuje fakt zmiany lub odebrania uprawnień do przetwarzania danych osobowych w prowadzonej ewidencji osób upoważnionych do przetwarzania danych osobowych w Urzędzie,
2) ABI bez zbędnej zwłoki blokuje lub zmienia profil użytkownika w systemie informatycznym.

4. Ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzi ABI.

ROZDZIAŁ III.

Metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem.

§ 9. Systemy informatyczne, w których przetwarzane są dane osobowe w Urzędzie wyposażone są w mechanizmy identyfikacji i uwierzytelniania. Każdorazowo, podczas uruchamiania aplikacji do przetwarzania danych osobowych, osoba uruchamiająca ją musi podać przypisany jej identyfikator. Po zaakceptowaniu identyfikatora, aplikacja przechodzi w tryb uwierzytelniania użytkownika. Po podaniu znanego jedynie użytkownikowi hasła uzyskuje on dostęp do danych osobowych.

§ 10. Procedura związana z zarządzaniem i użytkowaniem mechanizmów identyfikacji i uwierzytelniania – jest następująca:

1) w przypadku gdy do pracy w systemie informatycznym upoważnienia posiadają dwie osoby - system informatyczny zapewnia rejestrowanie odrębnego identyfikatora dla każdej z nich,
2) dostęp do danych – w przypadku jak w pkt. 1 – możliwy jest jedynie po podaniu identyfikatora przypisanego temu użytkownikowi oraz uwierzytelnieniu się w systemie,

3) identyfikatory użytkowników oraz wszelkie zmiany uprawnień dostępu do danych odnotowywane są przez ABI w ewidencji osób upoważnionych do przetwarzania danych osobowych w Urzędzie,
4) identyfikator użytkownika nie może być zmieniany chyba, że zaistnieją takie okoliczności jak włamanie do systemu, podglądnięcie przez osobę postronną itp. a po wyrejestrowaniu użytkownika z systemu nie może być przydzielany innej osobie,
5) użytkownik systemu informatycznego zobowiązany jest do zmiany hasła używanego do uwierzytelniania go w systemie informatycznym nie rzadziej niż co 30 dni,
6) hasła użytkowników muszą składać się z co najmniej sześciu znaków: literowych, cyfrowych lub innych,
7) identyfikatory i hasła użytkowników umożliwiające dostęp do systemu informatycznego, w którym przetwarzane są dane osobowe - objęte są tajemnicą służbową również po upływie czasu ich ważności,
8) bieżący nadzór nad funkcjonowaniem mechanizmów identyfikacji i uwierzytelniania użytkowników sprawuje ABI.

ROZDZIAŁ IV.
Procedury rozpoczęcia, zawieszenia i zakończenia pracy przez użytkowników systemów informatycznych.

§ 11. Właściwe użytkowanie systemu informatycznego wymaga realizacji przez użytkowników niżej wymienionych procedur rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym. W przypadku problemów z realizacją którejkolwiek z poniższych procedur, należy niezwłocznie powiadomić ABI.

§ 12. Procedura rozpoczęcia pracy w systemie informatycznym:
1) włączenie zasilacza awaryjnego UPS – odczekanie do momentu jego przejścia w stan gotowości do pracy,
2) włączenie komputera,
3) po załadowaniu się systemu operacyjnego – uruchomienie aplikacji do przetwarzania danych osobowych,
4) uzyskanie dostępu do systemu informatycznego następuje po pozytywnym uwierzytelnieniu identyfikatora użytkownika.

§ 13. Procedura zawieszenia pracy w systemie informatycznym:
4. wyjście z programu do przetwarzania danych osobowych,
5. wyłączenie monitora,
6. odpowiednie zabezpieczenie wydruków i innych materiałów zawierających dane osobowe.

§ 14. Procedura zakończenia pracy w systemie informatycznym:
1) dokonanie bezpiecznego opuszczenia programu do przetwarzania danych osobowych,
2) zakończenie pracy systemu operacyjnego,
3) bezpieczne wyłączenie komputera,
4) wyłączenie zasilacza awaryjnego UPS,

5) odpowiednie zabezpieczenie wydruków, nośników informacji oraz innych materiałów zawierających dane osobowe, używanych do pracy w systemie informatycznym.

ROZDZIAŁ V.

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

§ 15. Użytkownicy systemu informatycznego obowiązani są do okresowego tworzenia kopii zapasowych zbiorów danych. Zapasowe kopie zbiorów danych tworzy się jeden raz w tygodniu lub w miarę potrzeb – częściej.

§ 16. Kopie zbiorów danych zapisywane są na zewnętrznych nośnikach informacji (dyskietki, płyty CD – RW) z wyjątkiem płyt CD lub innych nośników jednorazowego zapisu.

§ 17. Procedura tworzenia kopii zapasowych zbiorów danych jest następująca:

1. do archiwizacji zbiorów danych osobowych używa się jedynie nośników danych dopuszczonych do obiegu wewnątrz Urzędu przez Podinspektora ds. obsługi informatycznej,
2. przejście w menu programu do przetwarzania danych osobowych do opcji tworzenia kopii baz danych,
3. umieszczenie nośnika informacji we właściwym napędzie (nośniki danych muszą być bezwzględnie sformatowane – pozbawione jakichkolwiek zapisów),
4. zapisanie na nośnik kopii baz danych,
5. sprawdzenie poprawności wykonania kopii baz danych,
6. w przypadku zapisywania na dyskietki 3,5'' należy po wykonaniu kopii dokonać ich zabezpieczenia przed zapisem (suwak w dolnej części dyskietki),
7. przenieść nośnik informacji z zapisaną kopią baz danych w miejsce ich przechowywania,
8. usunięcie z miejsca przechowywania „przestarzałej" kopii baz danych,
9. pozbawienie zapisu ww. nośnika i jego zwrot na stanowisko ds. obsługi informatycznej.

§ 18. W Urzędzie nie archiwizuje się programów oraz narzędzi programowych służących do przetwarzania danych osobowych.

§ 19. Ustala się następujące okresy rotacji nośników danych:

1) dla dyskietek – 10 zapisów,
2) dla płyt CD-RW oraz DVD-RW – do momentu zauważenia widocznych rys na płaszczyźnie roboczej dysku (ocena wizualna) lub uszkodzeń górnej części dysku (rysy, zadrapania, itp.).

§ 20. 1.Wycofanie nośników polega na ich zwrocie na stanowisko ds. obsługi informatycznej. Dyskietki i płyty nie muszą być likwidowane w przypadku zamkniętego obiegu nośników danych w Urzędzie.

2. Likwidacja musi być jednak przeprowadzona w przypadku, kiedy powyższy nośnik ulegnie zużyciu. Należy wówczas dyskietki – utylizować a płyty trwale zniszczyć w sposób mechaniczny. Przed likwidacją nośników należy je pozbawić wszelkiego rodzaju zapisów.

ROZDZIAŁ VI.

Sposób i miejsce przechowywania elektronicznych nośników informacji oraz kopii zapasowych zawierających dane osobowe.

§ 21. 1.W Urzędzie nie przechowuje się innych, niż zapasowe kopie baz danych, elektronicznych nośników informacji zawierających dane osobowe. Wyjątek stanowią awarie urządzeń komputerowych, które naprawia się „na miejscu". W przypadku braku takiej możliwości, przed oddaniem do naprawy, wymontowuje się z nich nośniki informacji (dyski twarde, pamięci). Jeżeli uszkodzeniu uległy te właśnie nośniki – dokonuje się komisyjnego ich zniszczenia.

2. Kopie zapasowe zbiorów danych oraz wyżej opisane nośniki przechowuje się w pancernej, ogniotrwałej szafie w pomieszczeniu innym niż to, w którym znajdują się systemy informatyczne.
3. Kopie zapasowe zbiorów danych przechowuje się do momentu utworzenia kolejnych.

ROZDZIAŁ VII.

Sposób zabezpieczenia systemów informatycznych przed działalnością wirusów komputerowych oraz innego szkodliwego oprogramowania.

§ 22. Biorąc pod uwagę fakt podstawowego poziomu bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych - sposób zabezpieczenia ich przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemów informatycznych polega na:

1) kontrolowanym obiegu nośników informacji wykorzystywanych na stanowiskach, na których przetwarzane są zbiory danych osobowych:
   a) dyskietki, płyty CD oraz inne nośniki informacji przychodzące z zewnątrz mogą być używane na ww. stanowiskach jedynie za zgodą inspektora ds. informacji elektronicznej,
   b) wprowadza się zamknięty obieg nośników informacji służących do tworzenia kopii zapasowych zbiorów danych (oznakowane i ponumerowane nośniki).

2) okresowym sprawdzaniu dysków komputerów, na których znajdują się zbiory danych osobowych oraz dyskietek używanych do tworzenia kopii zapasowych aktualnym programem antywirusowym, nie rzadziej niż raz w miesiącu.

§ 23. Obszarem systemu informatycznego narażonym na ingerencję wirusów oraz innego szkodliwego oprogramowania są stacje robocze stanowisk, na których przetwarzane są dane osobowe.

§ 24. Źródłami przedostania się szkodliwego oprogramowania do systemu może być używanie nie sprawdzonych nośników danych (dyskietek, płyt) nie dopuszczonych do obiegu przez inspektora ds. informacji elektronicznej.

§ 25. 1.W celu przeciwdziałania skutkom działania szkodliwego oprogramowania stosowany jest program antywirusowy NOD32.

2. Stacje robocze skanowane są programem antywirusowym raz w tygodniu.
3. Bazy antywirusowe aktualizowane są codziennie.

§ 26. W przypadku, gdy oprogramowanie zabezpieczające wskazuje zaistnienie zagrożenia związanego z działalnością szkodliwego oprogramowania, użytkownik ma obowiązek niezwłocznie poinformować o tym ABI, usuwając jednocześnie z napędów nośniki danych, z których doszło do domniemanego zainfekowania.

ROZDZIAŁ VIII.

Sposób realizacji wymogów w zakresie odnotowywania informacji o udostępnieniu danych osobowych.

§ 27. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system ten zapewnia automatyczne odnotowanie:

1) daty pierwszego wprowadzenia danych do systemu,
2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu,
3) źródła danych – w przypadku zbierania danych nie od osoby, której dane dotyczą,
4) informacji o odbiorcach, którym dane zostały udostępnione oraz dacie i zakresie tego udostępnienia,
5) wniesienia sprzeciwu wobec przetwarzania jej danych, o którym mowa w art. 32 ust. 1 pkt. 8 ustawy.

ROZDZIAŁ IX.

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

§ 28. 1.Systemy komputerowe oraz nośniki informacji służące do przetwarzania danych osobowych poddawane są regularnym przeglądom i konserwacjom w Urzędzie.

2. Odpowiedzialnym za dokonywanie ww. czynności jest inspektor ds. obsługi informatycznej.

§ 29. Procedura dotycząca wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych jest następująca:

1) przeglądów systemów służących do przetwarzania danych dokonuje się nie rzadziej niż raz na kwartał,
2) konserwacji systemów służących do przetwarzania danych dokonuje raz na pół roku,
3) przeglądów i konserwacji nośników informacji służących do przetwarzania danych dokonuje się raz w miesiącu.

§ 30. Czynności jakim należy poddać systemy służące do przetwarzania danych w celu przeprowadzenia:

1) przeglądu:
   a) dokonanie ogólnych oględzin stanu technicznego urządzeń,
   b) sprawdzenie systemu aktualnym programem antywirusowym,
   c) wykonanie standardowego sprawdzenia poprawności plików i folderów.

2) konserwacji:
   a) dokonanie szczegółowych oględzin stanu technicznego urządzeń systemu połączeń między nimi,
   b) gruntowne sprawdzenie aktualnym programem antywirusowym,
   c) wykonanie gruntownego sprawdzenia powierzchni dysku,
   d) wykonanie defragmentacji powierzchni dysku,
   e) usunięcie niepotrzebnych plików z folderów systemowych.

§ 31. Czynności jakim należy poddać nośniki informacji służące do przetwarzania danych w celu przeprowadzenia przeglądów i konserwacji:
1) dokonanie oględzin stanu technicznego nośników informacji,
2) sprawdzenie aktualnym programem antywirusowym,
3) wykonanie gruntownego sprawdzenia powierzchni nośników.

§ 32.W przypadku przekazywania do naprawy sprzętu komputerowego, na którym przetwarzane są dane osobowe, pozbawia się je twardych dysków i innych nośników danych. Dysków oraz innych (wymiennych) nośników danych nie naprawia się. Dane przegrywa się nowy nośnik, a uszkodzony po usunięciu, o ile jest to możliwe zapisów – należy niezwłocznie zniszczyć w sposób mechaniczny.

Załącznik Nr 3
do Zarządzenia Nr 176A/2009
Wójta Gminy Pątnów
z dnia 05 maja 2009 r.

INSTRUKCJA
postępowania w sytuacji naruszenia ochrony danych osobowych.

§ 1. Instrukcja przeznaczona jest dla osób zatrudnionych w Urzędzie, przy przetwarzaniu danych osobowych.

§ 2. Instrukcja określa tryb postępowania w sytuacjach; gdy:
1) stwierdzono naruszenie zabezpieczenia systemu informatycznego,
2) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy lub sposób działania programu mogą wskazywać na naruszenie zabezpieczenia danych.

§ 3. Naruszenie zabezpieczenia systemu informatycznego może polegać w szczególności na :
1) naruszeniu hasła dostępu (system nie reaguje lub je ignoruje – usunięty mechanizm hasła),
2) częściowym lub całkowitym braku bazy danych,
3) braku możliwości uruchomienia właściwego programu,
4) zmianie położenia sprzętu komputerowego lub możliwości połączenia wszystkich urządzeń,
5) kradzieży z pomieszczenia, w którym znajduje się sprzęt komputerowy.

§ 4. Każda osoba zatrudniona w Urzędzie, która stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych w systemie informatycznym, zobowiązana jest niezwłocznie poinformować o tym osobę zatrudnioną przy przetwarzaniu danych osobowych lub Administratora Bezpieczeństwa Informacji.

§ 5. Osoba zatrudniona przy przetwarzaniu danych osobowych, która uzyskała
1) informację lub sama stwierdziła naruszenie zabezpieczenia bazy danych osobowych w systemie informatycznym, zobowiązana jest niezwłocznie: zabezpieczyć pomieszczenie, w którym znajduje się sprzęt komputerowy,
2) powiadomić Administratora Bezpieczeństwa Informacji, a w przypadku jego nieobecności – Wójta.

§ 6. Administrator Bezpieczeństwa Informacji, po otrzymaniu zawiadomienia o naruszeniu bezpieczeństwa systemu informatycznego powinien niezwłocznie:

1) powiadomić Wójta,
2) w przypadku włamania lub kradzieży z pomieszczenia, w którym znajduje się komputer – powiadomić Policję,
3) przeprowadzić postępowanie wyjaśniające.

§ 7. W ramach prowadzonego postępowania wyjaśniającego – Administrator Bezpieczeństwa Informacji powinien w szczególności:

1. odnotować wszelkie informacje związane z tym wydarzeniem,
2) na bieżąco wygenerować i wydrukować (jeżeli zasoby systemu na to pozwalają) wszystkie możliwe dokumenty, które mogą pomóc w ustaleniu okoliczności zdarzenia,
3) sprawdzić stan urządzeń komputerowych, zawartość zbioru danych osobowych, sposób działania programu oraz możliwość obecności wirusów komputerowych,
4) podjąć działania w celu powstrzymania lub ograniczenia dostępu do danych osoby niepowołanej, zminimalizowania szkód i zabezpieczenia usunięciem śladów jej ingerencji poprzez:
    1. fizyczne odłączenie urządzeń, które mogły umożliwić dostęp do bazy danych osobie nieupoważnionej,
    2. zmianie hasła dostępu i identyfikatora użytkownika, przez które uzyskano nielegalny dostęp.

§ 8. 1. Po dokonaniu powyższych czynności – niezwłocznie należy przywrócić normalny stan działania systemu.

2. W przypadku zniszczenia, uszkodzenia lub nieuzasadnionej modyfikacji bazy danych, administrator bezpieczeństwa informacji wspólnie z osoba upoważnioną do przetwarzania danych osobowych spowoduje jej odtworzenie z ostatniej kopii awaryjnej.

§ 9. Z przeprowadzonego postępowania wyjaśniającego – Administrator Bezpieczeństwa Informacji – niezwłocznie sporządza protokół, który powinien zawierać:

1. opis zaistniałego zdarzenia,
2. metody dostępu do danych osoby nieupoważnionej,
3. skalę zniszczeń,
4. przyczyny naruszenia zabezpieczenia systemu informatycznego,
5. określenie działań mających zapobiec wystąpieniu podobnych zdarzeń w przyszłości,
6. wnioski o ukaranie w stosunku do pracowników, którzy swym zachowaniem spowodowali lub umożliwili naruszenie zabezpieczenia systemu informatycznego.

§ 10. 1. Protokół z przeprowadzonego postępowania – Administrator Bezpieczeństwa Informacji przedkłada Wójtowi najpóźniej w ciągu trzech dni od zaistniałego zdarzenia.

2. Na podstawie sporządzonego protokołu - Wójt Gminy podejmuje decyzję o realizacji zaproponowanych działań mających na celu wyeliminowanie możliwości naruszenia zabezpieczenia systemu informatycznego, a w szczególności:

1. jeżeli przyczyną zdarzenia był błąd osoby zatrudnionej przy przetwarzaniu danych osobowych w systemie informatycznym – należy przeprowadzić dodatkowe szkolenie wszystkich osób biorących udział przy przetwarzaniu danych,
2. jeżeli przyczyną zdarzenia było uaktywnienie wirusa – należy ustalić źródło jego pochodzenia oraz wykonać zabezpieczenie antywirusowe,
3. jeżeli przyczyną zdarzenia było włamanie w celu pozyskania bazy danych osobowych – należy dokonać szczegółowej analizy wdrożonych środków zabezpieczających w celu zapewnienia skuteczniejszej ochrony bazy danych,
4. jeżeli przyczyną zdarzenia był zły stan techniczny urządzenia lub sposób działania programu – należy niezwłocznie przeprowadzić czynności serwisowo – programowe,
5. jeżeli przyczyną zdarzenia było zaniedbanie ze strony osoby zatrudnionej przy przetwarzaniu danych osobowych – należy wyciągnąć konsekwencje służbowe lub skierować wniosek do organów ścigania.