Załącznik Nr 1
do zarządzenia Nr 36/07
Wójta Gminy Wiśniewo
z dnia 21 listopada 2007 roku

POLITYKA BEZPICZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH SYSTEMU INFORMTYCZNEGO URZĘDU GMINY W WIŚNIEWIE

Rozdział I
Zasady ogólne

§ 1

Ilekroć w niniejszym dokumencie jest mowa o:

a. Urzędzie – należy przez to rozumieć Urząd Gminy w Wiśniewie;

b. Administratorze Danych Osobowych – należy przez to rozumieć Wójta Gminy Wiśniewo;

c. Administratorze Bezpieczeństwa Informacji – należy przez to rozumieć pracownika urzędu lub inną osobę wyznaczoną do nadzorowania, przestrzegania zasad ochrony określonych w niniejszym dokumencie oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych;

d. Administratorze Systemu Informatycznego – należy przez to rozumieć osobę odpowiedzialną za funkcjonowanie systemu informatycznemu urzędu oraz stosowanie technicznych i organizacyjnych środków ochrony;

e. Użytkowniku systemu – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym urzędu. Użytkownikiem może być pracownik urzędu, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w urzędzie lub wolontariusz;

f. Sieci lokalnej – należy przez to rozumieć połączenie systemów informatycznych urzędu wyłącznie dla własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych;

g. Sieci rozległej – należy przez to rozumieć sieć publiczną w rozumieniu ustawy z dnia 1 lipca 2000 r. – Prawo Telekomunikacyjne (Dz.U. Nr 73, poz. 852 z późniejszymi zmianami).

§ 2

Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe wyznacza Administrator Bezpieczeństwa Informacji według wzoru określonego w **Załączniku nr 1** do niniejszego opracowania.

§ 3

1. Wykaz zbiorów danych osobowych przetwarzanych w systemie informatycznym prowadzi Administrator Bezpieczeństwa Informacji. Wykaz ten stanowi **Załącznik nr 2**.

2. W skład systemu wchodzą:
   a. dokumentacja papierowa (korespondencja, wnioski, deklaracje, itd.)
   b. urządzenia i oprogramowanie komputerowe służące do przetwarzania informacji oraz procedury przetwarzania danych w tym systemie, w tym procedury awaryjne
   c. wydruki komputerowe.

§ 4

Opisy struktur zbiorów danych osobowych oraz powiązań między zbiorami jak również sposób przepływu danych pomiędzy poszczególnymi systemami stanowi **Załącznik nr 3** do niniejszego opracowania.

§ 5

Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych:

1. Środki ochrony fizycznej:
   a. budynek urzędu, w którym zlokalizowany jest obszar przetwarzania danych osobowych jest wyposażony alarm;
   b. urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych zamkami patentowymi;
   c. drzwi wejściowe do urzędu oraz drzwi do pomieszczeń: USC i pomieszczenia serwera są antywłamaniowe;
   d. przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osoby zatrudnionej przy przetwarzaniu danych lub w obecności Administratora Bezpieczeństwa Informacji;
   e. pomieszczenia, o których mowa wyżej, powinny być zamykane na czas nieobecności pracownika zatrudnionego przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich;
   f. w przypadku przebywania interesantów bądź innych osób postronnych w pomieszczeniach, o których mowa wyżej, monitory stanowisk dostępu do danych osobowych powinny być ustawione a taki sposób, aby uniemożliwić tym osobom wgląd w dane;
   g. do przebywania w pomieszczeniu serwera uprawnieni są: Administrator Bezpieczeństwa Informacji, osoba odpowiedzialna za obsługę informatyczną urzędu oraz Administrator Danych;
   h. przebywanie w pomieszczeniu serwera osób nieuprawnionych dopuszczalne jest tylko w obecności jednej z osób upoważnionych, o których mowa w pkt. „g”.

2. Środki sprzętowe, informatyczne i telekomunikacyjne

a. każdy dokument papierowy zawierający dane osobowe przeznaczony do wyrzucenia powinien być zniszczony w sposób uniemożliwiający jego odczytanie, przy pomocy niszczarki, która umożliwia cięcie poprzeczne;
b. urządzenia wchodzące w skład systemu informatycznego podłączone są do odrębnego obwodu elektrycznego, zabezpieczonego na wypadek zaniku napięcia albo awarii w sieci zasilającej UPS-em;
c. siec lokalna podłączona do internetu;
d. na stanowiskach pracy, w których przetwarzane są dane osobowe zastosowano oprogramowanie do tworzenia kopii zapasowych;
e. na serwerze oraz w stacjach roboczych zainstalowano oprogramowanie antywirusowe, poczta elektroniczna wpływająca do Urzędu skanowana jest programem antywirusowym;
f. kopie awaryjne wykonywane są w cyklach:
   - tygodniowo na dysku twardym;
   - miesięcznie na płycie CD-R.

3. Środki ochrony w ramach oprogramowania systemu
   a. dostęp fizyczny do baz danych osobowych zastrzeżony jest wyłącznie dla osoby zajmującej się obsługą informatyczną urzędu, Administratora Bezpieczeństwa Informacji;
   b. konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych jedynie za pośrednictwem aplikacji;
   c. system informatyczny z jakiego korzystają pracownicy urzędu gminy pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu.

4. Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych
   a. zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji;
   b. dla każdego użytkownika systemu jest ustalony identyfikator;
   c. zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (unikalny identyfikator i hasło).

5. Środki ochrony w ramach systemu użytkowego
   a. zastosowano wygaszanie ekranu w przypadku dłuższej nieaktywności użytkownika;
   b. komputer, z którego możliwy jest dostęp do danych osobowych zabezpieczony jest hasłem uruchomieniowym (BIOS), hasłem wejściowym do systemu operacyjnego oraz hasłem do każdej aplikacji przy pomocy której przetwarzane są dane osobowe.

6. Środki organizacyjne
   a. osoby upoważnione do przetwarzania danych osobowych przed dopuszczeniem do pracy zostaną przeszkolone w zakresie obowiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz poinformowanie o podstawowych zagrożeniach związanych z przetwarzaniem danych w systemie informatycznym;
   b. prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych;
   c. wprowadzono instrukcję zarządzania systemem informatycznym;
   d. zdefiniowano procedury postępowania w sytuacji naruszenia ochrony danych osobowych;

e. wprowadzono obowiązek rejestracji wszystkich przypadków awarii systemu, działań konserwatorskich w systemie oraz naprawy systemu;
f. określono sposób postępowania z nośnikami informacji.

§ 6

Do zapoznania się z niniejszym dokumentem oraz stosowania zawartych w nim zasad zobowiązani są wszyscy pracownicy Urzędu upoważnieni do przetwarzania w systemie informatycznym.

Załącznik nr 1 do
Instrukcji Przetwarzania
Danych Osobowych

Wykaz

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

a) w Urzędzie Gminy

Lp.	Kondygnacja	Nr pokoju	Określenie zbioru danych
1.	I	1.	Ewidencja podatków i opłat lokalnych od osób fizycznych, prawnych i jednostek organizacyjnych nie posiadających osobowości prawnej
2.	I	2.	Rejestr świadczeniobiorców Gminnego Ośrodka pomocy Społecznej w Wiśniewie Rejestr osób pobierających stypendium socjalne Najem lokali mieszkalnych i użytkowych oraz dzierżawa
3.	I	3.	Osoby korzystające z pomocy Gminnej Komisji Rozwiązywania Problemów Alkoholowych w Wiśniewie
4.	I	4.	Rejestr podatników podatku od środków transportowych Rejestr pobranego podatku dochodowego od osób fizycznych oraz rozliczeń z zakresu ubezpieczeń społecznych Ewidencja działalności gospodarczej Zezwolenia na sprzedaż napojów alkoholowych
5.	I	6.	Gospodarka nieruchomościami Gminy Wiśniewo Zatwierdzenie planów zagospodarowania przestrzennego, wydawanie wypisów i wyrysów z planu zagospodarowania przestrzennego Numeracja porządkowa, zmiana numeracji porządkowej nieruchomości
6.	II	7.	Rejestracja przedpoborowych, sporządzanie list poborowych, przechowywanie książek ewidencji osób będących w FOC, akcja kurierska, świadczenia rzeczowe i osobiste Urząd Stanu Cywilnego w Wiśniewie Zbiór kart osobowych mieszkańca, dowody osobiste
7.	II	10.	Ewidencja skarg i wniosków

b) w Gminnej Bibliotece Publicznej

Lp.	Kondygnacja	Nr pokoju	Określenie zbioru danych
1	I	1	Kartoteka czytelników

Załącznik nr 2 do
Instrukcji Przetwarzania
Danych Osobowych

Wykaz zbiorów danych osobowych przetwarzanych w systemie informatycznym

- Zbiór kart osobowych mieszkańca, dowody osobiste;
- Zatwierdzenie planów zagospodarowania przestrzennego, wydawanie wypisów i wyrysów z planu zagospodarowania przestrzennego;
- Urząd Stanu Cywilnego w Wiśniewie;
- Rejestracja przedpoborowych, sporządzanie list poborowych, przechowywanie książek ewidencji osób będących w FOC, akcja kurierska, świadczenia rzeczowe i osobiste;
- Rejestr świadzczeniobiorców Gminnego Ośrodka pomocy Społecznej w Wiśniewie;
- Rejestr podatników podatku od środków transportowych;
- Rejestr pobranego podatku dochodowego od osób fizycznych oraz rozliczeń z zakresu ubezpieczeń społecznych;
- Rejestr osób pobierających stypendium socjalne;
- Osoby korzystające z pomocy Gminnej Komisji Rozwiązywania Problemów Alkoholowych w Wiśniewie;
- Numeracja porządkowa, zmiana numeracji porządkowej nieruchomości;
- Najem lokali mieszkalnych i użytkowych oraz dzierżawa;
- Kartoteka czytelników;
- Gospodarka nieruchomościami Gminy Wiśniewo;
- Ewidencja skarg i wniosków;
- Ewidencja działalności gospodarczej;
- Zezwolenia na sprzedaż napojów alkoholowych;
- Ewidencja podatków i opłat lokalnych od osób fizycznych, prawnych i jednostek organizacyjnych nie posiadających osobowości prawnej.

Załącznik nr 3 do
Instrukcji Przetwarzania Danych
Osobowych

Opisy struktur zbiorów danych osobowych

Lp.	Zbiory danych osobowych	Narzędzia do przetwarzania danych (program; firma)
1.	Zbiór kart osobowych mieszkańca, dowody osobiste	SEL-Win; ARAM
2.	Zatwierdzenie planów zagospodarowania przestrzennego, wydawanie wypisów i wyrysów z planu zagospodarowania przestrzennego	Word; Microsoft
3.	Urząd Stanu Cywilnego w Wiśniewie	USC
4.	Rejestracja przedpoborowych, sporządzanie list poborowych, przechowywanie książek ewidencji osób będących w FOC, akcja kurierska, świadczenia rzeczowe i osobiste	SEL-WIN; ARAM Word; Microsoft
5.	Rejestr świadzczeniobiorców Gminnego Ośrodka pomocy Społecznej w Wiśniewie	POMOST, Computerland
6.	Rejestr podatników podatku od środków transportowych	Podatki; CIOA
7.	Rejestr pobranego podatku dochodowego od osób fizycznych oraz rozliczeń z zakresu ubezpieczeń społecznych	Płatnik, PROKOM Płace, CIOA
8.	Rejestr osób pobierających stypendium socjalne	Świadczenia, Computerland
9.	Osoby korzystające z pomocy Gminnej Komisji Rozwiązywania Problemów Alkoholowych w Wiśniewie	Word; Microsoft
10.	Numeracja porządkowa, zmiana numeracji porządkowej nieruchomości	Word; Microsoft
11.	Najem lokali mieszkalnych i użytkowych oraz dzierżawa	Word; Microsoft
12.	Kartoteka czytelników	Kartoteka ręczna
13.	Gospodarka nieruchomościami Gminy Wiśniewo	Word; Microsoft
14.	Ewidencja skarg i wniosków	Word; Microsoft
15.	Ewidencja działalności gospodarczej	Word; Microsoft
16.	Zezwolenia na sprzedaż napojów alkoholowych	Word; Microsoft
17.	Ewidencja podatków i opłat lokalnych od osób fizycznych, prawnych i jednostek organizacyjnych nie posiadających osobowości prawnej	Podatki, CIOA

Załącznik Nr 2
do zarządzenia Nr 36/07
Wójta Gminy Wiśniewo
z dnia 21 listopada 2007 roku

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM URZĘDU GMINY W WIŚNIEWIE

Podstawa prawna:

- rozporządzenie 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 (Dz.U. Nr 100, poz. 1024)

- ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2002r, Nr 101, poz. 926 z późn. zm.).

§ 1

Ilekroć w niniejszym dokumencie jest mowa o:

a. Urzędzie – należy przez to rozumieć Urząd Gminy w Wiśniewie;

b. Administratorze Danych Osobowych – należy przez to rozumieć Wójta Gminy Wiśniewo;

c. Administratorze Bezpieczeństwa Informacji – należy przez to rozumieć pracownika urzędu lub inną osobę wyznaczoną do nadzorowania, przestrzegania zasad ochrony określonych w niniejszym dokumencie oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych;

d. Administratorze Systemu Informatycznego – należy przez to rozumieć osobę odpowiedzialną za funkcjonowanie systemu informatycznemu urzędu oraz stosowanie technicznych i organizacyjnych środków ochrony;

e. Użytkowniku systemu – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym urzędu. Użytkownikiem może być pracownik urzędu, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w urzędzie lub wolontariusz;

f. Sieci lokalnej – należy przez to rozumieć połączenie systemów informatycznych urzędu wyłącznie dla własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych;

g. Sieci rozległej – należy przez to rozumieć sieć publiczną w rozumieniu ustawy z dnia 1 lipca 2000 r. – Prawo Telekomunikacyjne (Dz.U. Nr 73, poz. 852 z późniejszymi zmianami).

§ 2

Procedury nadawania i zmiany uprawnień do przetwarzania danych:

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:
   a. Ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2002r, Nr 101, poz. 926 z późn. zm.);
   b. Polityką bezpieczeństwa danych osobowych systemu informatycznego;
   c. Niniejszym dokumentem.

2. Zapoznanie się z powyższymi informacjami pracownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi **Załącznik nr 1.**

3. Administrator Bezpieczeństwa Informacji przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnego upoważnienia administratora danych określającego zakres uprawnień pracownika, którego wzór stanowi **Załącznik nr 2.**

4. Bezpośredni nadzór nad przetwarzaniem danych osobowych w komórkach organizacyjnych Urzędu sprawują kierownicy tych komórek. Wzór upoważnienia określającego zakres odpowiedzialności stanowi **Załącznik nr 3.**

5. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora, hasła oraz zakresu dostępnych danych i operacji.

6. Hasło ustanowione podczas przyznawania uprawnień przez Administratora Bezpieczeństwa Informacji należy zmienić indywidualnie podczas pierwszego logowania się w systemie informatycznym. Ustanowione hasło, administrator przekazuje użytkownikowi ustnie.

7. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.

8. Pracownik ponosi pełną odpowiedzialność za wszystkie operacje wykonywane przy użyciu jego identyfikatora i hasła dostępu.

9. Wszystkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako naruszenie podstawowych obowiązków pracowniczych.

10. Pracownik zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest do zachowania ich w tajemnicy. Tajemnica obowiązuje go również po ustaniu zatrudnienia.

11. W systemie informatycznym stosuje się uwierzytelnienie dwustopniowe: na poziomie dostępu do sieci lokalnej oraz dostępu do aplikacji.

12. Identyfikator użytkownika w aplikacji (o ile działanie aplikacji na to pozwala), powinien być tożsamy z tym, jaki jest mu przydzielony w sieci lokalnej.

13. Odebranie uprawnień pracownikowi następuje na pisemny wniosek kierownika, któremu pracownik podlega z podaniem daty oraz przyczyny odebrania uprawnień. Wzór pisma o cofnięciu upoważnienia z pkt. 3 stanowi **Załącznik nr 4.**

14. Kierownicy komórek organizacyjnych zobowiązani są pisemnie informować Administratora Bezpieczeństwa Informacji o każdej zmianie dotyczącej podległych pracowników mającej wpływ na zakres posiadanych uprawnień w systemie informatycznym.

15. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane oraz unieważnić jej hasło.

16. Administrator Bezpieczeństwa Informacji zobowiązany jest do prowadzenia i ochrony rejestru użytkowników i ich uprawnień w systemie informatycznym.

17. Rejestr, którego wzór stanowi **Załącznik nr 5** powinien zawierać:
- imię i nazwisko użytkownika systemów informatycznych;
- numer uprawnienia;
- datę nadania uprawnienia;
- datę odebrania uprawnienia;
- przyczynę odebrania uprawnienia;
- podpis Administratora Bezpieczeństwa Informacji.

18. Rejestr powinien odzwierciedlać aktualny stan systemu w zakresie użytkowników i ich uprawnień oraz umożliwiać przeglądanie historii zmian uprawnień użytkowników.

§ 3

Zasady posługiwania się hasłami:
1. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła;

2. Hasło użytkownika powinno być zmieniane co najmniej raz w miesiącu;

3. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie;

4. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł;

5. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności;

6. Pracownik nie ma prawa do udostępniania haseł danej grupy osobom spoza tej grupy, dla której zostały one utworzone;

7. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie;

8. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła;

9. Przy wyborze hasła obowiązują następujące zasady
   a. minimalna długość hasła – 6 znaków;
   b. zakazuje się stosować:
      - haseł, które użytkownik stosował uprzednio w okresie minionego roku,
      - swojej nazwy użytkownika w jakiejkolwiek formie (pisanej dużymi literami, w odwrotnym kierunku, dublując każda literę, itp.),
      - ogólnie dostępnych informacji o użytkowniku takich jak: numer telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego, nazwa ulicy na której mieszka lub pracuje, itp.
      - wyrazów słownikowych,
      - przewidywalnych sekwencji znaków z klawiatury np.: „QWERTY”, „12345678”, itp.
   c. należy stosować:
      - hasła zawierające kombinacje liter i cyfr,
      - hasła zawierające znaki specjalne: znaki interpunkcyjne, nawiasy, symbole @, #, &, itp. o ile system informatyczny na to pozwala,
      - hasła, które można zapamiętać bez zapisywania,
      - hasła łatwe i szybkie do wprowadzenia, po to by trudniej było podejrzeć je osobom trzecim.

10. Zmiany hasła nie wolno zlecać innym osobom;

11. W systemach, które umożliwiają opcję zapamiętywania nazw użytkownika lub jego hasła nie należy korzystać z tego ułatwienia;

12. Hasło użytkownika o prawach administratora powinno znajdować się w zalakowanej kopercie w zamykanej na klucz szafie metalowej, do której dostęp mają:
    - Administrator Bezpieczeństwa Informacji;
    - Kierownik urzędu lub osoba przez niego wyznaczona.

§ 4

Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie:

1. Przed rozpoczęciem pracy w systemie komputerowym należy zameldować się do systemu przy użyciu indywidualnego identyfikatora oraz hasła;

2. Przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wykonać operację wylogowania z systemu;

3. Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązana jest wykonać funkcję wylogowania z systemu;

4. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów, wykonać zamknięcie systemu i jeżeli jest to konieczne wymeldować się z sieci komputerowej;

5. Niedopuszczalne jest wyłączenie komputera przed zamknięciem oprogramowania oraz zakończeniem pracy w sieci;

§ 5

Procedury tworzenia zabezpieczeń:

1. Za systematyczne przygotowywanie kopii bezpieczeństwa odpowiada Administrator Bezpieczeństwa Informacji, a w przypadku jego nieobecności Administrator Systemu Informatycznego;

2. Kopie bezpieczeństwa wykonywane są raz na miesiąc po zakończeniu pracy wszystkich użytkowników sieci komputerowej;

3. Zabezpieczenie wszystkich programów i danych wykonywane jest w pierwszym tygodniu po 15 dniu każdego miesiąca w postaci zapisu na płycie CD-R lub CD-RW;

4. Płyty CD-R lub CD-RW przechowuje się w sejfie urzędu;

5. W przypadku wykonywania zabezpieczeń długoterminowych lub dyskietkach lub płytach CD-R (CD-RW), nośniki te należy co kwartał sprawdzać pod kątem ich dalszej przydatności.

§ 6

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz wydruków:

1. Elektroniczne nośniki informacji:
   a. dane osobowe w postaci elektronicznej – za wyjątkiem kopii bezpieczeństwa – zapisywane na dyskietkach, dyskach magnetooptycznych czy dyskach twardych nie są wynoszone poza siedzibę urzędu;
   b. wymienne elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych, określony w Polityce bezpieczeństwa przetwarzania danych osobowych urzędu;
   c. po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki są przechowywane w zamykanych szafach biurowych lub kasetkach;
   d. urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
   e. urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi nieuprawnionemu do otrzymywania danych osobowych pozbawia się wcześniej zapisu tych danych;
   f. urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej.

2. Kopie zapasowe:
   a. kopie zapasowe zbioru danych osobowych oraz oprogramowania i narzędzi programowych zastosowanych do przetwarzania danych są przechowywane w sejfie urzędu;

b. dostęp do ww. sejfu maja tylko upoważnieni pracownicy.

3. Wydruki:
   a. w przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym;
   b. pomieszczenie, w którym przechowywane są wydruki robocze musi być należycie zabezpieczone po godzinach pracy;
   c. wydruki, które zwierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

§ 7

Środki ochrony systemu przed złośliwym oprogramowaniem, w tym wirusami komputerowymi:

1. Na każdym stanowisku komputerowym oraz serwerze musi być zainstalowane oprogramowanie antywirusowe pracujące w trybie monitora;

2. Każdy e-mail wpływający do urzędu musi być sprawdzony pod kątem występowania wirusów przez bramkę antywirusową;

3. Definicje wzorców wirusów aktualizowane są nie rzadziej niż raz w miesiącu;

4. Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje użytkownik, który nośnik zamierza użyć;

5. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik;

6. Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje pracownik, który pocztę otrzymał;

7. Administrator Systemu Informatycznego przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach;

8. Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania;

9. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe na którym wirusa wykryto oraz wszystkie posiadane przez użytkownika nośniki informacji.

§ 8

Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych:

1. Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie osobom upoważnionym;

2. Udostępnienie danych osobowych, w jakiejkolwiek postaci, jednostkom nieuprawnionym wymaga pisemnego upoważnienia Administratora Danych;

3. Udostępnienie danych osobowych nie może być realizowane droga telefoniczną.

4. Udostępnienie danych osobowych może nastąpić wyłącznie po przedstawieniu wniosku o udostępnienie danych osobowych. Wniosek powinien zawierać informacje:
   a. o podstawie prawnej wniosku
   b. umożliwiające wyszukanie w zbiorze żądanych danych
   c. wskazanie ich zakresu
   d. o przeznaczeniu danych;

5. Pracownik, który udostępnia dane osobowe ma obowiązek prowadzenia rejestrów udostępnionych danych osobowych, który musi zawierać co najmniej: datę udostępnienia, podstawę, zakres udostępnionych informacji oraz osobę lub instytucję dla której dane udostępniono;

§ 9

1. Użytkownik systemu informatycznego zobowiązany jest zawiadomić administratora bezpieczeństwa informacji za pośrednictwem informatyka o każdym naruszeniu zabezpieczenia systemu polegającym na:
   a. naruszeniu hasła dostępu (system nie reaguje na hasło lub je ignoruje – usunięty mechanizm hasła);
   b. częściowym lub całkowitym braku bazy danych;
   c. braku możliwości uruchomienia właściwej aplikacji (programu komputerowego);
   d. zmianie położenia sprzętu komputerowego lub możliwości połączenia wszystkich urządzeń

2. Administrator bezpieczeństwa informacji, po otrzymaniu zawiadomienia o naruszeniu zabezpieczenia systemu informatycznego powinien niezwłocznie:
   a. przeprowadzić postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia ochrony danych osobowych;
   b. podjąć działania zabezpieczające system przed ponownym naruszeniem;
   c. sporządzić raport z naruszenia bezpieczeństwa systemu informatycznego **Załącznik nr 6**.

3. Raport, o którym mowa w § 9 pkt. 2 lit. c, przekazuję się niezwłocznie, jednakże nie później niż w ciągu 3 dni administratorowi danych osobowych.

4. W przypadku kradzieży sprzętu informatycznego z pomieszczeń, użytkownik niezwłocznie powiadamia bezpośredniego przełożonego.

5. W sytuacji, o której mowa w § 9 pkt. 4, bezpośredni przełożony zobowiązany jest do niezwłocznego powiadomienia Administratora Bezpieczeństwa Informacji.

6. Informatyk jest zobowiązany na bieżąco informować administratora bezpieczeństwa informacji o przypadkach awarii programowych wynikających z:
   a. posługiwania się przez użytkowników nieautoryzowanymi programami;
   b. nie przestrzegania zasad używania programów antywirusowych w określonych okolicznościach;
   c. niewłaściwego wykorzystywania sprzętu komputerowego

7. Administrator bezpieczeństwa informacji składa okresowo, nie rzadziej niż raz na rok, administratorowi danych osobowych, kompleksową analizę zarządzania systemem informatycznym służącym przetwarzaniu danych osobowych oraz założenia strategii i polityki zabezpieczenia systemów informatycznych.

§ 10

1. Dokumenty systemu informatycznego, w szczególności zawierające opis parametrów technicznych oraz rozwiązania systemowe, zapewniające ochronę poufności, integralności i rozdzielczości są informacją niejawną oznaczoną klauzulą „poufne".

2. Dokumenty, o których mowa w ust.1 są przygotowywane i wdrażane przez Administratora Bezpieczeństwa Informacji.

Załącznik nr 1 do
Instrukcji Zarządzania
Systemem Informatycznym

O Ś W I A D C Z E N I E

Oświadczam, że zapoznałem/łam się z przepisami prawa dotyczącymi ochrony danych osobowych, a w szczególności z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002r. Nr 101 poz. 926 z późn. zm.) oraz z Zarządzeniem Nr 36/07 Wójta Gminy Wiśniewo z dnia 21 listopada 2007r. i zobowiązuję się do przestrzegania tajemnicy danych osobowych, a w szczególności:

- zachowania szczególnej staranności w trakcie wykonywania operacji przetwarzania danych w celu ochrony interesów osób, które one dotyczą,
- zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym.

Oświadczam ponadto, że zapoznałem/łam się z:

- zasadami postępowania przy przetwarzaniu danych osobowych,
- instrukcją określającą sposób postępowania w przypadku zaistnienia podejrzenia naruszenia zabezpieczeń przetwarzanych w systemie danych osobowych,
- instrukcją określającą sposób zarządzania systemem informatycznym,
- polityką bezpieczeństwa

stanowiącymi załączniki do Zarządzenia Nr 36/07 Wójta Gminy Wiśniewo z dn. 21 listopada 2007r.

Świadomy/ma odpowiedzialności porządkowej i karnej znane mi dane osobowe zachowam w tajemnicy, również w sytuacji gdyby ustało moje zatrudnienie w Urzędzie Gminy w Wiśniewie.

....

data podpis pracownika

Załącznik nr 2 do
Instrukcji Zarządzania
Systemem Informatycznym

U P O W A Ż N I E N I E Nr

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002r. nr 101, poz. 926 z późn. zm.),

u p o w a ż n i a m

Pana/Panią .....
Zatrudnioną.....
na stanowisku .....
.....

do przetwarzania danych osobowych, wynikającego z zakresu obowiązków pracowniczych.

.....
/Podpis Pracodawcy/

.....
/data i podpis pracownika/

Załącznik nr 3 do
Instrukcji Zarządzania
Systemem Informatycznym

U P O W A Ż N I E N I E Nr

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U.z 2002 nr 101 poz. 926 z późn. zm.)

u p o w a ż n i a m

Pana/Panią .....

.....

stanowisko służbowe

do przetwarzania danych osobowych gromadzonych w związku z realizacją przydzielonych obowiązków pracowniczych

zobowiązuję:

1. do zastosowania niezbędnych środków technicznych i organizacyjnych określonych w przepisach powszechnie obowiązujących, w celu zapewnienia ochrony przetwarzania danych osobowych w podległym wydziale,
2. do kontroli przestrzegania zasad i sposobu wykonywania operacji przetwarzania danych przez podległych pracowników.

powierzam:

Odpowiedzialność w zakresie przestrzegania zasad i ochrony danych osobowych w Urzędzie Gminy w Wiśniewie.

.....

/Podpis /

.....

/data i podpis pracownika/

Załącznik nr 4 do
Instrukcji Zarządzania
Systemem Informatycznym

W y c o f a n i e u p o w a ż n i e n i a

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002r. nr 101, poz. 926 z późn. zm.).

W związku z:

.....

.....

..... .

cofam upoważnienie

Pana/Pani .....
zatrudnionego/zatrudnionej w .....
.....
na stanowisku .....
.....

do przetwarzania danych osobowych, wynikającego z zakresu obowiązków pracowniczych.

.....
/Podpis Pracodawcy/

.....
/data i podpis pracownika/

Załącznik nr 5 do
Instrukcji Zarządzania
Systemem Informatycznym

Rejestr użytkowników i ich uprawnień w systemie informatycznym

Nr uprawnienia	Imię i nazwisko	Data nadania	Data odebrania	Przyczyna odebrania	Podpis Administratora Bezpieczeństwa Informacji

Załącznik nr 6 do
Instrukcji Zarządzania
Systemem Informatycznym

R A P O R T
z naruszenia bezpieczeństwa systemu bezpieczeństwa w Urzędzie Gminy w Wiśniewie

1. Data: …….. Godzina: ……
   (dd.mm.rrrr) (00:00)
2. Osoba powiadamiająca o zaistniałym zdarzeniu:

   ……...
   (Imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje))
3. Lokalizacja zdarzenia

   ……...
   (np. nr pokoju, nazwa pomieszczenia)
4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

   .....

   .....

   .....
5. Podjęte działania:

   .....

   .....

   .....
6. Przyczyny wystąpienia zdarzenia:

   .....

   .....

   .....
7. Postępowanie wyjaśniające:

   .....

   .....

   .....

……..
Data, podpis Administratora Bezpieczeństwa Informacji