Zarządzenie Wójta Gminy Bargłów Kościelny nr 8/06
z dnia 10-02-2006r.

w sprawie: **wprowadzenia do użytku służbowego polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Bargłowie Kościelnym.**

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

§ 1

1. Wprowadza się do użytku służbowego „Politykę bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Bargłowie Kościelnym" w brzmieniu stanowiącym załącznik nr 1 do zarządzenia.

2. Wprowadza się do użytku służbowego „Instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy w Bargłowie Kościelnym" w brzmieniu stanowiącym załącznik nr 2 do zarządzenia.

§ 2

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

§ 3

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

§ 4

Zarządzenie wchodzi w życie z dniem podjęcia.

Załącznik nr 1
do Zarządzenia Wójta nr 8/06
z dn. 10-02-2006r.

„Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy w Bargłowie Kościelnym„

§ 1

1. Celem polityki bezpieczeństwa jest takie postępowanie, aby osoby upoważnione do przetwarzania danych osobowych w pełni zabezpieczyły dostęp do nich przed osobami nieupoważnionymi oraz gromadziły je w zbiorach zgodnie z wymogami ustawy o ochronie danych osobowych (Dz. U. Nr 101 poz. 926 z 2002r.)

2. Polityką bezpieczeństwa objęte są dane osobowe w rozumieniu ustawy o ochronie danych osobowych.

3. Reguły i zasady do przetwarzania danych osobowych prowadzonych zarówno w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych obowiązują, także w przypadku przetwarzania danych poza zbiorem danych.

4. Całokształt działań należy traktować jako ochronę prywatności osób, których dane są przetwarzane oraz jako wymóg ustawowy.

§ 2

Integralną część polityki bezpieczeństwa stanowią niniejsze postanowienia:

1) Wykaz pomieszczeń stanowiących obszar w którym przetwarzane są dane osobowe, zawarty jest w wykazie nr 1 tworzącym integralną część niniejszego dokumentu.

2) Budynek posiada następujące zabezpieczenia:

- wewnętrzny system alarmowy (pomieszczenia kasowe, korytarze),
- ustalony wewnętrzny system zabezpieczenia pomieszczeń
- ustalony sposób zabezpieczenia dokumentów (zamki patentowe, szafy metalowe);

3) Wykaz zbiorów danych osobowych stanowi wykaz nr 2 tworzący integralną cześć niniejszego dokumentu.

§ 3

Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności i integralności przetwarzanych danych zostały określone w „Instrukcji zarządzania systemami informatycznymi służącym do przetwarzania danych osobowych w Urzędzie Gminy Bargłów Kościelny”.

§ 4

Zobowiązuję wszystkie osoby posiadające upoważnienie do przetwarzania danych osobowych, nadane przez administratora danych, do bezwzględnego przestrzegania podanych w niniejszym opracowaniu reguł i zasad tworzących politykę bezpieczeństwa.

Wykaz nr 1
do Polityki bezpieczeństwa
systemów informatycznych

Wykaz pomieszczeń w których przetwarzane są dane osobowe w Urzędzie Gminy w Bargłowie Kościelnym

W budynku Urzędu Gminy w Bargłowie Kościelnym, ulica Augustowska 47, pomieszczeniami w których przetwarzane są dane osobowe w formie kartotek, rejestrów i stacjonarnego sprzętu komputerowego są pomieszczenie:

- Podatki i Opłaty: 9
- Księgowość Finansowa: 7
- USC, Dowody osobiste, Ewidencja ludności: 10
- Referat Finansowo Księgowy, Księgowość Bodżetowa Oświaty: 12

Wykaz nr 2
do Polityki Bezpieczeństwa systemów informatycznych

Wykaz zbiorów danych osobowych przetwarzanych w systemach informatycznych w Urzędzie Gminy w Bargłowie Kościelnym

1. Podatki -
   - podatki od osób fizycznych
   - podatki od osób prawnych

     U.I. Infosystem s.c. (podatki, księgowość zobowiązań)
2. Ewidencja Ludności -
   - dowody osobiste – IDL SYSTEM
   - Ewidencja ludności – SELWIN ARAM
   - USC – ESOUSC KOMPLEX-SERVICE
3. Płace -
   - Płace U.I. Infosystems s.c.
   - Dokumenty ZUS – Program Płatnik
   - NFOS

Załącznik nr 2
do Zarządzenia Wójta nr 8/06
z dn. 10-02-2006r.

„Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy w Bargłowie Kościelnym”

Rozdział 1

Postanowienia ogólne

§ 1

Niniejsza Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy w Bargłowie Kościelnym zwana dalej „instrukcją” określa ogólne zasady zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy w Bargłowie Kościelnym.

§ 2

Przetwarzanie danych osobowych w Urzędzie Gminy w Bargłowie Kościelnym opiera się na zasadach określonych w ustawie z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity Dz.U. Nr 101, poz.926 z późniejszymi zmianami).

Rozdział 2

Objaśnienia

§3

Przez użyte w instrukcji określenia należy rozumieć:

1) dane osobowe – wszelkie informacje o określonej lub dającej się określić osobie fizycznej;

2) dane osobowe powszechnie dostępne – informacje dotyczące osoby fizycznej zawarte w rejestrach jawnych tj. dostępnych z mocy prawa dla osób trzecich;

3) zbiór danych – każdy posiadający strukturę zestaw danych o charakterze osobowym dostępny wg określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

4) przetwarzanie danych – jakiekolwiek operacje wykonywane na danych osobowych zarówno w systemach informatycznych jaki i metodami tradycyjnymi (kartoteki, księgi, wykazy);

5) administrator danych – Wójt Gminy Bargłów Kościelny;

.

6) administrator bezpieczeństwa informacji – osoba odpowiedzialna za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń. Osoba ta powoływana jest zarządzeniem Wójta;

7) administrator systemu – osoba wyznaczona przez Wójta Gminy, odpowiedzialna za sprawność i konserwację oraz wdrożenie technicznych zabezpieczeń systemów informatycznych w Urzędzie Gminy w Bargłowie Kościelnym

8) kierownik komórki organizacyjnej – Kierownik referatu, w którym zatrudniony jest pracownik przetwarzający dane oraz samodzielnie pracujące osoby w komórkach jednoosobowych;

9) bezpośredni przełożony – osoba sprawująca bezpośredni nadzór nad pracownikiem;

10) Urząd – Urząd Gminy w Bargłowie Kościelnym.

§4

Naruszenie ochrony danych osobowych, może być spowodowane:

1) niekontrolowanym działaniem osób trzecich, powodującym zakłócenia systemu podczas włamania, niewłaściwym działaniem zespołów serwisowych, przetwarzaniem danych osobowych bez uprawnień, tworzeniem w zbiorach użytkownika nieautoryzowanych kont dostępu;

2) umyślnym lub nieumyślnym działaniem, a nawet zaniechaniem działania użytkowników przetwarzających dane osobowe lub osób odpowiedzialnych za ich ochronę.

3) niewłaściwym oddziaływaniem czynników zewnętrznych, takich jak: temperatura otoczenia, wilgotność, pole elektromagnetyczne, wirusy komputerowe, skutki powodzi, pożaru, itp.;

§5

Za naruszenie ochrony danych osobowych uważa się w szczególności:

1) brak możliwości fizycznego dostępu do danych np. zagubiony klucz do pomieszczenia, lub mebli biurowych, w których przechowywane są dokumenty, zniszczona szafa z dokumentami, brak nośników informacji, zalane pomieszczenie, brak sprzętu komputerowego itp.;

2) brak dostępu do zawartości zbioru danych – zbiór istnieje lecz nie można go otworzyć;

3) zmienioną zawartość zbioru, niepoprawną treść, postać, data, różnicę w danych itp.;

4) próbę lub fakt nieuprawnionego dostępu do zbioru danych lub pomieszczenia w którym jest przetwarzany np. zmiana ułożenia kolejności dokumentów, otwarte drzwi lub meble biurowe, nietypowe ustawienie sprzętu lub pojawienie się nowych dokumentów;

5) różnicę funkcjonowania systemu, a w szczególności wyświetlania komunikatów i informacji o błędach oraz nieprawidłowościach w wykonywaniu operacji;

6) zniszczenie lub próby zniszczenia, w sposób nieautoryzowany danych ze zbioru lub danych systemowych;

7) zmianę lub utratę danych zapisanych na kopiach awaryjnych lub zapisach archiwalnych;

8) nieskuteczne niszczenie nośników informacji zawierających dane osobowe (dyskietki, nośniki optyczne, wydruki papierowe), umożliwiające ponowny ich odczyt przez osoby nieuprawnione;

9) próba nielegalnego logowania się do systemu lub włamania do systemu;

10) zmienione oprogramowanie systemu, stwierdzone przez użytkownika po przerwie w przetwarzaniu danych.

Rozdział 3

Obowiązki pracownicze wynikające z ochrony danych osobowych

§ 6

1. Obowiązek przestrzegania tajemnicy danych osobowych dotyczy wszystkich pracowników, którzy mają dostęp do informacji o charakterze danych osobowych.

2. Naruszenie zasad ochrony danych osobowych, w efekcie którego nastąpiło udostępnienie danych osobie nie upoważnionej, jest **ciężkim naruszeniem obowiązków pracowniczych**.

3. Kierownicy komórek organizacyjnych Urzędu są zobowiązani do:

1) zastosowania niezbędnych środków technicznych i organizacyjnych, określonych w przepisach powszechnie obowiązujących w celu zapewnienia ochrony przetwarzania danych osobowych;

2) kontroli przestrzegania zasad i sposobu wykonywania operacji przetwarzania danych przez podległych pracowników;

3) sygnalizowania niezgodności aktów prawnych oraz aktów wewnętrznych Urzędu z przepisami ustawowymi w zakresie ochrony danych osobowych i przedstawienia stosownych projektów zmian, mających na celu ich dostosowanie do regulacji ustawowej;

4) zwracania się do administratora danych, w przypadku istotnych wątpliwości co do stosowania przepisów prawych z zakresu ochrony danych osobowych

4. Czynności przetwarzania danych osobowych może dokonywać jedynie pracownik upoważniony przez administratora danych, w zakresie indywidualnych obowiązków pracowniczych.

5. Osoba upoważniona przez administratora danych osobowych, jest zobowiązana do:

1) zapoznania się z przepisami prawa w zakresie ochrony danych osobowych;

2) stosowania określonych przez administratora danych procedur i środków, mających na celu zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym;

3) zachowania szczególnej staranności w trakcie wykonywania operacji przetwarzania danych w celu ochrony interesów osób, których dane dotyczą;

4) podporządkowanie się poleceniom kierownika komórki organizacyjnej i przestrzegania ustalonych przez niego szczegółowych zasad i procedur.

Rozdział 4

Postępowanie przy upoważnianiu osób do przetwarzania danych osobowych

§ 7

1. W przypadku przyjęcia do pracy nowego pracownika, którego zakres obowiązków obejmować będzie przetwarzanie danych osobowych, Administrator danych wydaje upoważnienie do przetwarzania danych osobowych.

2. Pracownik, któremu administrator danych udzieli upoważnienia, jest zobowiązany do podpisania oświadczenia, którego treść stanowi załącznik nr 1.

3. Przepisy ustępu 1, 2, 4, 5 i 6 stosuje się odpowiednio do stażystów odbywających staż w Urzędzie.

4. W przypadku zmiany stanowiska przez pracownika, bądź zakresu obowiązków pracowniczych, kierownik komórki organizacyjnej i samodzielne stanowisko pracy zobowiązani są bezzwłocznie powiadomić Administratora Danych o zaistniałej sytuacji.

5. Wypowiedzenie umowy o pracę przez pracodawcę jest równocześnie cofnięciem upoważnienia administratora do przetwarzania danych.

6. W sytuacji wypowiedzenia umowy o pracę przez pracownika, upoważnienie traci moc z datą rozwiązania umowy o pracę.

7. Ewidencję pracowników upoważnionych do przetwarzania danych prowadzi Referat Organizacyjny.

8. W ewidencji pracowników winny znaleźć się następujące dane: nazwisko i imię, identyfikator, stanowisko, referat, w którym pracownik jest zatrudniony, wskazanie zbiorów danych, do których pracownik ma prawo dostępu, data przyznania uprawnień, data wyrejestrowania pracownika z systemu informatycznego.

Rozdział 5

Postępowanie w przypadku utworzenia nowego zbioru danych osobowych

§ 8

1. W przypadku konieczności utworzenia nowego zbioru danych, wynikającej z obowiązków nałożonych przepisami ustawy bądź nowymi zasadami, kierownik komórki organizacyjnej i samodzielne stanowisko pracy zobowiązani są niezwłocznie – nie później niż w ciągu 7 dni – poinformować o tym fakcie administratora danych.

2. Informacja, o której mowa w ust. 1 powinna zawierać:

   1) nazwę zbioru (ewidencji);
   2) podstawę prawną utworzenia nowego zbioru danych;
   3) metodę katalogowania (system komputerowy, metoda tradycyjna);
   4) zakres danych zawartych w zbiorze (np. imię, nazwisko, PESEL);
   5) sposób zbierania danych osobowych;
   6) podmioty, którym dane osobowe będą udostępniane.

Rozdział 6

Postępowanie w przypadku naruszenia zasad ochrony danych osobowych

§ 9

1. W przypadku uzasadniającego podejrzenia naruszenia zasad ochrony danych osobowych w Urzędzie, pracownik zobowiązany jest do niezwłocznego poinformowania o tym kierownika komórki organizacyjnej.

2. Kierownik komórki organizacyjnej, po dokonaniu oceny stanu faktycznego i stwierdzeniu naruszenia, jest zobowiązany poinformować o tym fakcie administratora danych oraz administratora bezpieczeństwa informacji.

3. W przypadku powtarzającego się naruszenia zasad ochrony danych osobowych, pracownik jest zobowiązany do niezwłocznego poinformowania administratora danych o tym fakcie.

Rozdział 7

Zasady udostępniania i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych.

§ 10

1. W systemie informatycznym odnotowywane są informacje o odbiorcach danych z tego systemu. Jeśli system informatyczny tego nie umożliwia, informacje odnotowywane są w formie papierowej.

2. Odbiorcą danych jest każdy, komu udostępnia się dane osobowe, z wyłączeniem:
   1) osoby, której dane dotyczą,
   2) osoby użytkownika systemu lub innej osoby upoważnionej do przetwarzania danych osobowych w urzędzie,
   3) podmiotu, któremu powierzono przetwarzanie danych,
   4) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

3. Odnotowanie obejmuje informacje o:
   1) nazwie jednostki organizacyjnej lub imieniu i nazwisku osoby, której udostępniono dane,
   2) zakresie udostępnianych danych,
   3) dacie udostępnienia.

4. Obowiązek odnotowania ww. informacji spoczywa na użytkowniku systemu, w tym celu wypełnia on odpowiednie pole w bazie danych osobowych.

   1) Odnotowanie informacji powinno nastąpić niezwłocznie po udostępnieniu danych.
   2) Udostępnienie danych osobowych może nastąpić wyłącznie na pisemną prośbę odbiorcy danych.
   3) Na żądanie osoby, której dane zostały udostępnione, informacje o udostępnieniu danych są zamieszczane w raporcie z systemu informatycznego lub wyciągu z rejestru papierowego, a raport przekazywany jest tej osobie.

4) Nadzór nad prawidłowością odnotowywania w systemie ww. informacji sprawuje Administrator Bezpieczeństwa Informacji.

§ 11

1. Wprowadza się następujące zasady udostępniania danych osobowych:

   1) w obiegu wewnętrznym między referatami, informacje zawierające dane powszechnie dostępne może udostępnić pracownik przetwarzający dane w formie bezpośredniej lub telefonicznie

   2) zgodę na udostępnianie danych osobowych w szerszym zakresie, w obiegu wewnętrznym między referatami, wyraża kierownik komórki organizacyjnej;

   3) w obiegu zewnętrznym zgodę na udostępnienie danych osobowych wyraża administrator danych lub osoba przez niego upoważniona, zgodnie z przepisami powszechnie obowiązującymi.

Rozdział 8

Ogólne zasady eksploatacji systemów komputerowych i systemów przetwarzania danych osobowych

§ 12

1. Dane osobowe z użyciem systemu informatycznego są przetwarzane w godzinach pracy Urzędu, poza tymi godzinami wyłącznie w uzasadnionych przypadkach, po uzyskaniu pisemnej zgody administratora danych i powiadomieniu administratora bezpieczeństwa informacji.

2. W obszarze przetwarzania danych osobowych mogą przebywać wyłącznie pracownicy zatrudnieni przy przetwarzaniu danych, osoby zainteresowane przetwarzanymi danymi, administrator bezpieczeństwa informacji, administrator systemu informatycznego oraz inne osoby indywidualnie upoważnione do tego przez administratora danych. Przebywanie osób nieuprawnionych do dostępu do danych osobowych w pomieszczeniach znajdujących się wewnątrz obszaru przetwarzania tych danych, jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych.

3. Pomieszczenia w obszarze przetwarzania danych osobowych muszą być zamykane na zamek w czasie nieobecności pracowników. Klucze powinny być przechowywane w sposób uniemożliwiający dostęp do nich przez osoby nieupoważnione do przetwarzania danych osobowych.

4. Monitory komputerów na których odbywa się przetwarzanie danych osobowych muszą być zlokalizowane w sposób uniemożliwiający osobom trzecim widok wyświetlanych danych.

5. Ekrany monitorów komputerów na których odbywa się przetwarzanie danych osobowych muszą być automatycznie wyłączane po upływie 5 minut nieaktywności użytkownika.

6. Dyski i inne nośniki elektroniczne zawierające dane osobowe a przeznaczone do likwidacji, naprawy lub przekazania podmiotowi nieuprawnionemu do otrzymania danych, są przed oddaniem pozbawiane zapisu.

7. Wydruki komputerowe zawierające dane osobowe, a przeznaczone do likwidacji, są w ciągu dnia gromadzone na stanowiskach pracy i na koniec dnia niszczone w sposób uniemożliwiający ich odczytanie, np. w niszczarce dokumentów.

8. Zabronione jest wykorzystywanie systemów informatycznych do celów niezgodnych z przeznaczeniem, a w szczególności instalowania gier oraz oprogramowania innego niż niezbędne do realizacji przetwarzania danych i/lub realizacji innych zadań służbowych

9. Zabronione jest samowolne instalowanie i używanie programów komputerowych; programy komputerowe instalowane są przez administrator systemu lub za jego zgodą przez inną upoważnioną osobę. Każdy z pracowników zobowiązany jest podpisać oświadczenie o odpowiedzialności za legalności oprogramowania na powierzonym mu komputerze – załącznik
nr 2.

10. Zabronione jest używania nośników danych udostępnionych przez osoby nieuprawnione, używania nośników danych niewiadomego pochodzenia lub niezwiązanych z pracą

11. Zabronione jest udostępnianie osobom nieuprawnionym możliwości dostępu do sieci wewnętrznej lub Internetu na stanowisku przetwarzającym dane osobowe;

12. Zabronione jest wykonywanie kopii danych osobowych oraz wydruków danych osobowych w celach innych niż wynikające z zasad przetwarzania danych, archiwizacji i/lub przekazanie danych podmiotowi uprawnionemu.

13. Wydruki komputerowe i nośniki danych zawierające dane osobowe muszą być przechowywane w zamkniętych szafach, w sposób uniemożliwiający ich odczytanie przez osoby nieuprawnione.

Rozdział 9

Nadawanie i cofanie uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

§ 13

1. Osobą odpowiedzialną za nadawanie i cofanie uprawnień jest administrator systemów informatycznych

2. W Urzędzie administratorem systemów informatycznych jest osoba pracująca na stanowisku: Informatyka. Może ona pełnić również funkcję „Administratora Bezpieczeństwa Informacji”

2. W przypadku umów serwisowych, administratorem systemu może być tez przedstawiciel firmy obsługującej program / system komputerowy.

3. Nadawanie uprawnień do przetwarzania danych osobowych i rejestrowanie uprawnień w systemie informatycznym odbywa się na polecenie Administratora Danych, po uprzednim wydaniu pisemnego upoważnienia.

4. Pracownik którego zakres obowiązków obejmuje dostęp i pracę w systemie informatycznym w którym przetwarzane są dane osobowe otrzymuje od administratora systemów informatycznych

Urzędu (bądź przedstawiciela firmy zewnętrznej w przypadku umowy serwisowej i obsługi systemu przez firmę zewnętrzną):

1) uprawnienia do pracy w systemie, a w szczególności unikalny identyfikator i hasło z możliwością samodzielnej zmiany (jeśli system informatyczny to umożliwia);

2) login (identyfikator) i hasło - z możliwością zmiany i ważnością 30 dni - do pracy w sieci komputerowej, jeśli system do przetwarzania danych osobowych znajduje się w sieci komputerowej i to umożliwia;

3) hasło do komputera - hasło BIOS - jeśli komputer udostępnia taką funkcję.

§ 14

1. W przypadku gdy pracownik Urzędu zmienił stanowisko pracy bądź ustał stosunek pracy, jego indywidualne hasła i uprawnienia do pracy przy przetwarzaniu danych osobowych są wycofywane przez:

1) skasowanie konta użytkownika;

2) zmianę uprawnień odpowiednich do zakresu obowiązków.

Rozdział 10

Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

§ 15

1. W Urzędzie stosuje się następujące metody i środki uwierzytelniania:

1. zabezpieczenie na poziomie BIOS'u komputera – indywidualne hasło komputera pozwalające włączyć komputer w celu załadowania systemu operacyjnego;

2. login i hasło do systemu operacyjnego, jeśli system operacyjny komputera posiada wbudowany mechanizm uwierzytelniania.

3. login i hasło do pracy w sieci komputerowej, jeśli sieć komputerowa posiada mechanizm uwierzytelniania

4. inne metody uwierzytelniania stosowane w miarę potrzeb (np. karty mikroprocesorowe, metody biometryczne)

2. Każdy użytkownik systemu jest zobowiązany nie udostępniać nikomu swoich haseł dostępu, nie przechowywać ich zapisanych w widocznym i łatwo dostępnym miejscu.

3. W każdej komórce Urzędu rejestr haseł dostępu do komputerów - hasła BIOS - przechowuje
Kierownik komórki. Indywidualne hasła użytkowników nie są ujawniane.

§ 16

1. Hasła dostępu (oprócz hasła BIOS) muszą składać się co najmniej z 6 znaków, hasło zawiera małe i wielkie litery oraz cyfry lub znaki specjalne

2. Hasła dostępu są zmieniane samodzielnie przez użytkownika lub pod nadzorem administratora systemu, przez użytkownika na polecenie administratora bezpieczeństwa informacji, który jest odpowiedzialny za te czynności:

1) do programów - co 30 dni automatycznie, chyba że funkcja taka nie jest zaimplementowana w programie, wtedy zmiana następuje ręcznie, lub w przypadku naruszenia bezpieczeństwa, chyba że odrębne przepisy wymagają ważności hasła przez określony czas;

2) do systemu operacyjnego (i/lub sieci komputerowej) – co 30 dni automatycznie, chyba że funkcja taka nie jest zaimplementowana w systemie, wtedy zmiana następuje ręcznie, lub w przypadku naruszenia bezpieczeństwa, chyba że odrębne przepisy wymagają ważności hasła przez określony czas;

3) w przypadku innych metod uwierzytelniania, zgodnie z odpowiednimi instrukcjami do systemów, nie rzadziej jednak niż co 30 dni.

Rozdział 11

Procedury rozpoczęcia i zakończenia pracy oraz pracy po zaniku napięcia

§ 17

1. Rozpoczynając pracę na komputerze użytkownik podaje wszystkie wymagane identyfikatory i hasła w sposób uniemożliwiający ich ujawnienie innym osobom.

2. Ustawienie monitora powinno uniemożliwiać podgląd osobom nieuprawnionym, szczególnie w procesie obsługi klienta.

3. W przypadku opuszczenia stanowiska pracy, użytkownik systemu obowiązany jest uruchomić wygaszacz ekranu, wyłączyć monitor lub w inny sposób uniemożliwić podgląd danych w czasie swojej nieobecności

4. Po zakończeniu pracy użytkownik powinien prawidłowo wylogować się z systemu, wyłączyć komputer.

5. W przypadku zaniku napięcia, które ma charakter trwały, użytkownik powinien:

1) jeśli system wyposażony jest w zasilacz awaryjny (UPS), - natychmiast zapisać dane, wylogować się z systemu i bezpiecznie wyłączyć komputer;

2) w innym przypadku, po przywróceniu zasilania i ponownym włączeniu komputera, należy skontrolować prawidłowe funkcjonowanie system, w razie wątpliwości przed kontynuacją pracy powiadomić administratora systemu.

6. W przypadku serii krótkich zaników napięcia (np. sygnalizowane dźwiękiem przez zasilacz awaryjny) należy zakończyć pracę oraz powiadomić osoby odpowiedzialne za budynek o niestabilności sieci energetycznej oraz powiadomić administratora systemu, który określi czy zasilacz jest sprawny.

Rozdział 12

Procedury tworzenia kopii zapasowych zbiorów danych

§ 18

1. Kopie bezpieczeństwa systemów wykonywane są w cyklu miesięcznym.

   Wykonuje się kopie :

   - programów płacowo-kadrowych
   - ewidencji podatkowej
   - innych zbiorów danych osobowych

2. Kopie wykonuje się na trwałych nośnikach takich jak dyskietki, płyty CD, płyty DVD

3. Kopie bezpieczeństwa są sprawdzane automatycznie pod względem poprawności zapisu danych.

4. Kopie bezpieczeństwa należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia danych w przypadku awarii systemu.

5. Wykonanie kopii nie jest obowiązkowe jeżeli w danym okresie nie wykonano zapisu zmieniającego bazę danych

Rozdział 13

Sposób, miejsce i okres przechowywania nośników elektronicznych i kopii bezpieczeństwa

§ 19

1. Elektroniczne nośniki danych i kopie bezpieczeństwa przechowuje się w pomieszczeniach do których mają dostęp tylko uprawnione osoby do przetwarzania danych osobowych .

2. Elektroniczne nośniki przechowuje się w zamkniętych ma klucz szafach w zabezpieczonych pudełkach lub innym opakowaniu które chroni przed kurzem i wilgocią.

3. Po okresie przydatności kopii zapasowych lub po ich uszkodzeniu nośnik danych przekazuje się do fizycznej likwidacji.

Rozdział 14

Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania wirusowego

§ 20

1. Ochrona antywirusowa jest realizowana przez oprogramowanie antywirusowe instalowane na komputerach użytkowników.

2. Oprogramowanie antywirusowe jest systematycznie uaktualniane automatycznie lub co najmniej raz w miesiącu przez administratora systemu.

3. Wszystkie dyskietki, których zawartość jest wczytywana do komputera muszą być każdorazowo sprawdzane programem antywirusowym. Odpowiedzialnym za te czynności jest pracownik obsługujący komputer.

4. Każdorazowo po pojawieniu się komunikatu o wykryciu wirusa należy bezzwłocznie zawiadomić o tym fakcie przełożonego oraz administratora systemu.

5. Użytkownik komputera, w którym jest zainstalowany program antywirusowy, zobowiązany jest do sprawdzenia całego komputera na obecność wirusów komputerowych przynajmniej raz w miesiącu.

Rozdział 15

Konserwacja i naprawa systemu przetwarzającego dane osobowe

§ 21

1. Prace dotyczące przeglądów, konserwacji i napraw wymagające zaangażowania autoryzowanych firm zewnętrznych, są wykonywane przez uprawnionych przedstawicieli tych firm – serwisantów - pod nadzorem administratora systemu lub osoby przez niego upoważnionej.

2. W wypadku konieczności wymiany gwarancyjnej nośnika na którym przechowywane są dane osobowe, dane wymazywane są w trwały sposób przez administratora systemu lub - jeśli nie jest to możliwe w ramach Urzędu - przez specjalistyczną firmę.

3. Urządzenia komputerowe, dyski twarde lub inne informatyczne nośniki danych, przeznaczone do naprawy, pozbawia się przed naprawą zapisu danych osobowych w sposób trwały - jeśli nie jest to możliwe w ramach Urzędu, korzysta się ze specjalistycznej firmy - lub naprawia się je pod nadzorem administratora systemu lub osoby przez niego upoważnionej.

Rozdział 16

Zasady postępowania z komputerami przenośnymi

§ 22

1. Komputery przenośne, używane do przetwarzania danych osobowych, powinny być zabezpieczone podczas transportu oraz przechowywania przed dostępem do tych danych osób nieuprawnionych, w szczególności należy:

1) zabezpieczyć dostęp do komputera na poziomie systemu operacyjnego – poprzez obligatoryjne wprowadzenie nazwy użytkownika i hasła

2) zabezpieczyć dostęp do komputera hasłem na poziomie BIOS

3) nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych;

Rozdział 17

Przepisy końcowe

§ 23

„Instrukcja“ ma zastosowanie na wszystkich stanowiskach pracy, na których przetwarzane są dane osobowe w Urzędzie oraz na innych stanowiskach wskazanych przez administratora bezpieczeństwa informacji, w zakresie przez niego wyznaczonym (np. podłączonych do wspólnej sieci komputerowej).

§ 24

1. Każdy użytkownik przetwarzający dane osobowe w zbiorach Urzędu Gminy w Bargłowie Kościelnym zobowiązany jest zapoznać się z niniejszą Instrukcją i stosować przepisy w niej zawarte na swoim stanowisku pracy.

2. Nadużycie przez użytkownika postanowień niniejszej Instrukcji może stanowić podstawę do pociągnięcia go do odpowiedzialności dyscyplinarnej, odszkodowawczej lub karnej, w trybie i na zasadach przewidzianych przepisami prawa.

§ 25

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

Załącznik nr 1
do Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy w Bargłowie Kościelnym

.....
(imię i nazwisko pracownika)

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

O Ś W I A D C Z E N I E

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

1. Ustawy z dni 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz. U. z
2002 r. Nr 101 poz. 926 z późn. zm.).

2. Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. nr 100, poz. 1024).

3. Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Bargłowie Kościelnym

4. Instrukcji określającej sposób zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych w Urzędzie Gminy w Bargłowie Kościelnym.

Jednocześnie w czasie wykonywania swoich obowiązków służbowych zobowiązuję się do:

a) zapewnienia ochrony danym osobowym przetwarzanym w zbiorach Urzędzie Gminy w Bargłowie Kościelnym, a w szczególności zapewnienia ich bezpieczeństwa przed udostępnianiem osobom trzecim i nieuprawnionym, zabraniem, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem,

b) zachowaniem w tajemnicy, także po ustaniu stosunku pracy, wszelkich informacji dotyczących funkcjonowania systemów lub urządzeń służących do przetwarzania danych osobowych w zbiorach Urzędu Gminy w Bargłowie Kościelnym,

c) zachowania w tajemnicy hasła dostępu do systemów informatycznych, przetwarzających dane osobowe w Urzędzie Gminy w Bargłowie Kościelnym, również po upływie jego ważności,

d) natychmiastowego zgłaszania przełożonemu i Administratorowi Bezpieczeństwa Informacji stwierdzenia na swoim stanowisku pracy, próby lub faktu naruszenia zabezpieczenia fizycznego pomieszczenia, bezpieczeństwa zbioru lub systemu informatycznego, w którym przetwarzane są dane osobowe.

Bargłów Kościelny, dnia ....
(podpis pracownika ubiegającego się o dostęp)

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

Załącznik nr 2
do Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy w Bargłowie Kościelnym

/WZÓR/

Komputer:
Nr inwentarzowy:

Miejsce zainstalowania:

OŚWIADCZENIE
o odpowiedzialności za powierzony sprzęt komputerowy

Po przeprowadzonej kontroli w dniu ..... oświadczam, iż oprogramowanie zainstalowane na komputerze wymienionym powyżej jest w pełni legalne.

.....
/ podpis Informatyka/

Oświadczam, iż powierzony mi sprzęt komputerowy będzie wykorzystywany zgodnie z jego przeznaczeniem oraz biorę pełną odpowiedzialność za legalność zainstalowanego na nim oprogramowania.

Bargłów Kościelny dn. ..... podpis.....
/Data, Imię Nazwisko, podpis pracownika/

- Na powierzonym komputerze może być wykorzystywane wyłącznie oryginalne, licencjonowane oprogramowanie, zainstalowane przez informatyka lub za jego wiedzą.
- Nie wolno instalować, kopiować, uruchamiać programów nielicencjonowanych (z dysku, dyskietki, CD-ROM'u lub innego nośnika).
- Nie wolno kopiować i przechowywać na dysku komputera plików i programów niezwiązanych z wykonywanymi obowiązkami służbowymi, w szczególności dotyczy to: plików muzycznych i filmowych łamiących prawa autorskie, programów rozrywkowych (gry, komunikatory internetowe itp.)
- Wszelkie wątpliwości związane z legalnością oprogramowania należy wyjaśniać z informatykiem.