ZARZĄDZENIE NR 49/07

WÓJTA GMINY KUŹNICA

z dnia 26 września 2007 roku

w sprawie zatwierdzenia „Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy Kuźnica" oraz „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Kuźnica".

Na podstawie art. 33 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (Dz. U. z 2001 roku Nr 142, poz. 1591 z późn. zm.) w związku z art. 36 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 roku Nr 101, poz. 926, Nr 153, poz. 1271, z 2004 roku Nr 25, poz. 219, Nr 33, poz. 285 oraz z 2006 roku Nr 104, poz. 708 i 711) zarządza się co następuje:

§ 1. 1. Zatwierdza się "Politykę bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy Kuźnica" stanowiącą Załącznik Nr 1 do niniejszego zarządzenia.

1. Powyższy dokument znajduje odpowiednio zastosowanie dla Systemu Obsługi Obywatela (SOO).

2. Zatwierdza się "Instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Kuźnica" stanowiącą Załącznik Nr 2 do niniejszego zarządzenia.

3. Powyższy dokument znajduje odpowiednio zastosowanie dla Systemu Obsługi Obywatela (SOO).

§ 2. Zarządzenie wchodzi w życie z dniem podpisania.

inż. Jan Kuźniakowski

07-09-26 14:25

Załącznik Nr 1

do Zarządzenia Nr 49/07

Wójta Gminy Kuźnica

z dnia 26 września 2007 roku

POLITYKA BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCHW URZĘDZIE GMINY KUŹNICA

Wprowadzenie

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych w Urzędzie Gminy Kuźnica zwanym dalej „Urzędem".

Opisane reguły określają granice dopuszczalnego zachowania wszystkich. użytkowników systemów informatycznych wspomagających pracę Urzędu. Dokument zwraca uwagę na konsekwencje jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

Odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi współczesnym systemom informatycznym.

Dokument „Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy Kuźnica", zwany dalej "Polityką bezpieczeństwa", wskazujący sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w systemach informatycznych, przeznaczony jest dla osób zatrudnionych przy przetwarzaniu tych danych.

Potrzeba jego opracowania wynika z rozporządzenia Prezesa Rady Ministrów z dnia 25 sierpnia 2005 roku w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr 171, poz. 1433) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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).

1. "Polityka bezpieczeństwa" określa tryb postępowania w przypadku, gdy:

1) stwierdzono naruszenie zabezpieczenia systemu informatycznego,

2) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci informatycznej mogą wskazywać na na ruszenie zabezpieczeń tych danych.

2. "Polityka bezpieczeństwa" obowiązuje wszystkich pracowników Urzędu.

3. Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemach informatycznych Urzędu.

4. Administrator danych, którym jest Wójt wyznacza Administratora Bezpieczeństwa Informacji danych zawartych w systemach informatycznych Urzędu, zwanego dalej "Administratorem Bezpieczeństwa".

5. "Administrator Bezpieczeństwa" realizuje zadania w zakresie ochrony danych, a w szczególności:

1) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Urzędu,

2) podejmowania stosownych działań zgodnie z niniejszą "Polityką bezpieczeństwa" w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym,

3) niezwłocznego informowania Wójta o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,

4) nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych,

6. Osoba zastępująca Administratora Bezpieczeństwa powyższe zadania realizuje w przypadku nieobecności Administratora Bezpieczeństwa.

7. Osoba zastępująca składa Administratorowi Bezpieczeństwa relację z podejmowanych działań w czasie jego zastępstwa. Niniejszy dokument jest zgodny z następującymi aktami prawnymi:

1) ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 roku Nr 101, poz. 926 z późn. zm.),

2) ustawą o ochronie informacji niejawnych z dnia 22 stycznia 1999 roku (Dz. U. Nr 11, poz. 95 z późn. zm.),

3) rozporządzeniem Prezesa Rady Ministrów z dnia 25 lutego 1999 roku w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. z 2005 roku Nr 171, poz. 1433),

4) rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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 I

OPIS ZDARZEŃ NARUSZAJACYCH OCHRONĘ DANYCH OSOBOWYCH

1. Podział zagrożeń:

1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i

uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych.

2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufuości danych.

3) zagrożenia zamierzone, świadome i celowe – najpoważniejsze zagrożenia, naruszenia poufuości danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na:

- nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
- nieuprawniony dostęp do systemu z jego wnętrza (osoby trzecie),
- nieuprawniony przekaz danych,
- bezpośrednie zagrożenie materialnych składników systemu.

2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:

1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej, itp.,

2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,

3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,

4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,

5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,

6) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,

7) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),

8) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,

9) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,

10) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych – np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,

11) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp.,

12) podmieniono lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe,

13) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej, itp..

ROZDZIAŁ II

ZABEZPIECZENIE DANYCH OSOBOWYCH

1. Administratorem danych osobowych zawartych i przetwarzanych w systemach informatycznych Urzędu jest Wójt Gminy.

2. Administrator danych osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych Urzędu, a w szczególności:

1) zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,

2) zapobiegać przed zabraniem danych przez osobę nieuprawnioną,

3) zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.

3. Do zastosowanych środków technicznych należy:

1) przetwarzanie danych osobowych w wydzielonych pomieszczeniach położonych w strefie administracyjnej,

2) zabezpieczenie wejścia do pomieszczeń, o których mowa w pkt 1,

3) wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji.

4. Do zastosowanych środków organizacyjnych należą przede wszystkim następujące zasady:

1) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy przetwarzaniu danych osobowych,

2) przeszkolenie osób, o których mowa w pkt l, w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych,

3) kontrolowanie otwierania i zamykania pomieszczeń, w których są przetwarzane dane osobowe, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę.

5. Niezależnie od niniejszych zasad opisanych w dokumencie "Polityka bezpieczeństwa", w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne

regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy zadań osób zatrudnionych przy przetwarzaniu danych osobowych w określonym systemie.

6. Wykaz pomieszczeń w których przetwarzane są dane osobowe oraz opis systemów informatycznych Urzędu i ich zabezpieczeń zawiera Załącznik Nr 1 do niniejszego dokumentu.

ROZDZIAŁ III

KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Wójt Gminy oraz "Administrator Bezpieczeństwa Informacji" sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.

2. Administrator Bezpieczeństwa sporządza roczne plany kontroli zatwierdzone przez Wójta i zgodnie z nimi przeprowadza kontrole oraz dokonuje rocznej oceny stanu bezpieczeństwa danych osobowych.

3. Na podstawie zgromadzonych materiałów, o których mowa w ust. 2, Administrator Bezpieczeństwa sporządza roczne sprawozdanie i przedstawia Wójtowi Gminy.

ROZDZIAŁ IV

POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. W przypadku stwierdzenia naruszenia:

1) zabezpieczenia systemu informatycznego,

2) technicznego stanu urządzeń,

3) zawartości zbioru danych osobowych,

4) ujawnienia metody pracy lub sposobu działania programu,

5) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,

6) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.),

każda osoba zatrudniona przy przetwarzaniu danych osobowych jest obowiązana niezwłocznie powiadomić o tym fakcie Administratora Bezpieczeństwa.

2. W razie niemożliwości zawiadomienia Administratora Bezpieczeństwa lub osoby przez niego upoważnionej, należy powiadomić bezpośredniego przełożonego.

3. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Bezpieczeństwa lub upoważnionej przez niego osoby, należy:

1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,

2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,

3) zaniechać – o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,

4) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,

5) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,

6) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,

7) udokumentować wstępnie zaistniałe naruszenie,

8) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa lub osoby upoważnionej.

4. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Administrator Bezpieczeństwa lub osoba go zastępująca:

1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Urzędu,

2) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszemem,

3) rozważa celowość i potrzebę powiadamia o zaistniałym naruszeniu Administratora danych,

4) nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza Urzędu dokumentuje zaistniały przypadek naruszenia oraz sporządza raport według wzoru stanowiącego Załącznik Nr 2, który powinien zawierać w szczególności:

1) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,

2) określenie czasu i miejsca naruszenia i powiadomienia,

3) określenie okoliczności towarzyszących i rodzaju naruszenia,

4) wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,

5) wstępną ocenę przyczyn wystąpienia naruszenia,

6) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

5. Raport, o którym mowa w ust. 6 Administrator Bezpieczeństwa niezwłocznie przekazuje Wójtowi Gminy, a w przypadku jego nieobecności osobie uprawnionej.

6. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu Administrator Bezpieczeństwa zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.

7. Zaistniałe naruszenie może, stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Wójta Gminy i Administratora Bezpieczeństwa Informacji.

8. Analiza, o której mowa w ust. 9, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

ROZDZIAŁ V

POSTANOWIENIA KOŃCOWE

1. Wobec osoby: która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentyjącego ten przypadek, wszczyna się postępowanie dyscyplinarne.

2. Administrator Bezpieczeństwa zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych według wzoru stanowiącego Załącznik Nr 3 do niniejszego dokumentu.

3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez. osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym Administratora Bezpieczeństwa.

4. Orzeczona kara: dyscyplinarna, wobec osoby uchylającej się od powiadomienia administratora bezpieczeństwa informacji nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 roku Nr 101, poz. 926) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

5. W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 roku Nr 101, poz. 926), rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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) oraz rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 roku w sprawie sposobu technicznego przygotowania systemów i sieci do przekazywania informacji do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposopów zabepieczenia danych informatycznych (Dz. U. Nr 100, poz. 1023).

Załącznik Nr 1

do Polityki bezpieczeństwa
systemów informatycznych
służących do przetwarzania
danych osobowych w Urzędzie
Gminy Kuźnica

z dnia 26 września 2007 roku

WYKAZ POMIESZCZEŃ, W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE, OPIS SYSTEMÓW INFORMATYCZNYCH W URZĘDZIE GMINY KUŹNICA

1. Wykaz pomieszczeń, w których przetwarzane są dane osobowe:

Komórka organizacyjna	System
Skarbnik, Podatki	Windows XP Professional
Ewidencja ludności , Dowody osobiste	Windows XP Professional

2. Wykaz zbiorów danych osobowych oraz programy zastosowane do przetwarzania tych danych.

Nazwa zbioru (opis)	Program do przetwarzania
UG Płace	Płace INFO-SYSTEM
UG ZUS	Płatnik PROKOM Software S. A.
UG Podatki	Podatki INFO-SYSTEM
UG System Ewidencji Ludności	SEL WIN
UG Dowody osobiste	WASKO S. A.

3. W celu ochrony przed utratą danych w Urzędzie Gminy zastowane są następujące zabezpieczenia:

1) odrębne zasilanie sprzętu komputerowego,

2) ochrona komputerów przed zanikiem zasilania poprzez stosowanie zasilaczy awaryjnych (UPS).

4. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu:

1) Aby uzyskać dostęp do zasobów sieci, należy zwrócić się do Wójta Gminy z odpowiednim wnioskiem, w którym podane będą dane nowego 4 użytkownika oraz zasoby jakie ma on mieć udostępnione.

2) W systemie informatycznym Urzędu zastosowano podwójną autoryzację użytkownika. Pierwszej autoryzacji należy dokonać w momencie włączenia komputera, podając hasło.

Drugiej autoryzacji należy dokonać uruchamiając program użytkowy, podając login użytkownika i hasło. Dostęp do wybranej bazy danych Urzędu uzyskuje się dopiero po poprawnym podwójnym zalogowaniu się do systemu informatycznego Urzędu.

5. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu poprzez Internet. W zakresie dostępu z sieci wewnętrznej Urzędu do sieci rozległej Internet zastosowano środki ochrony przed penetrowaniem i atakiem z zewnątrz..

Zastosowano również system wykrywający obecność wirusów w poczcie elektronicznej.

W efekcie zapewnione jest:

1) filtrowanie pakietów i blokowanie niektórych usług,

2) objęcie ochroną antywirusową wszystkich danych ściąganych z Internetu na stacjach lokalnych.

6. Postanowienia końcowe.

1) Do pomieszczeń, w których następuje przetwarzanie danych osobowych mają dostęp uprawnione osoby bezpośrednio związane z nadzorem nad komputerami lub aplikacjami.

2) Zabezpieczenie przed nieuprawnionym dostępem do danych, prowadzone jest przez Wójta Gminy, zgodnie z przyjętymi procedurami nadawania uprawnień do systemu informatycznego.

3) Osoby mające dostęp do danych powinny posiadać zaświadczenie o przebytym szkoleniu z zakresu ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997roku (Dz. U. Nr 133, poz. 883 z późn. zm).

4) W budynku znajdują się gaśnice, które okresowo są napełniane i kontrolowane przez specjalistę.

Załącznik Nr 2

do Polityki bezpieczeństwa
systemów informatycznych
służących do przetwarzania
danych osobowych w Urzędzie
Gminy Kuźnica

z dnia 26 września 2007 roku

Wzór

RAPORT

z naruszenia bezpieczeństwa systemu informatycznego w Urzędzie Gminy Kuźnica

1. Data ..... godzina .....

2. Osoba powiadamiająca o zaistniałym zdarzeniu (imię i nazwisko, stanowisko, nazwa użytkownik, jeśli występuje): .....
.....

3. Lokalizacja zdarzenia (numer pokoju, nazwa pomieszczenia): .....
.....

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące .....
.....
.....
.....

5. Podjęte działania: .....
.....
.....
.....

6. Przyczyny wystąpienia zdarzenia: .....
.....
.....
.....

7. Postępowanie wyjaśniające: .....
.....
.....
.....

.....

data i podpis

Administratora Bezpieczeństwa Informacji

07-09-26 14:25

Załącznik Nr 3

do Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy Kuźnica

z dnia 26 września 2007 roku

Wzór

WYKAZ OSÓB, KTÓRE ZOSTAŁY ZAPOZNANE Z "POLITYKĄ BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE GMINY KUŹNICA" PRZEZNACZONEJ DLA OSÓB ZATRUDNIONYCH PRZY PRZETWARZANIU TYCH DANYCH

Przyjąłem/ęłam do wiadomości i stosowania zapisy Polityki bezpieczeństwa

Imię i nazwisko	Komórka organizacyjna	Data i podpis

Załącznik Nr 2

do Zarządzenia Nr 49/07

Wójta Gminy Kuźnica

z dnia 26 września 2007 roku

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI SŁUŻĄCYMI DO PRZETWARZANIA DANYCH OSOBOWYCH URZĘDU GMINY KUŹNICA

Część ogólna

§ 1. Każdy petent Urzędu Gminy Kuźnica ma prawo do ochrony dotyczących jego danych osobowych.

§ 2.

1. Za dane osobowe uważa się każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby.

2. Dane osobowe są przechowywane:

1) w systemach informatycznych (mogą być nimi również pojedyncze komputery),

2) w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych.

§ 3. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:

1) zezwalają na to przepisy prawa,

2) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,

3) jest niezbędne do wypełnienia usprawiedliwionych, celów administratorów danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą.

§ 4. Z uwagi na ochronę interesów osób, których dane dotyczą, zapewnia się:

1) przetwarzanie danych zgodnie z prawem,

2) zbieranie danych dla oznaczonych, zgodnie z prawem celów i nie poddawanie ich dalszemu przetwarzaniu niezgodnemu z tymi celami,

3) poprawność merytoryczną danych i ich adekwatność w stosunku do celów, w jakich są przetwarzane,

przechowywanie danych w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Część szczegółowa

§ 5. Administratorem danych jest Wójt Gminy.

§ 6. Administrator danych wyznacza administratora bezpieczeństwa informacji, czyli odpowiedzialną za bezpieczeństwo danych osobowych w systemie informatycznym, a szczególnie 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.

§ 7.

1. Ustala się, że w Urzędzie Gminy Kuźnica obszar, w którym przetwarza się dane w następujących pokojach:

1) Pokój Nr – (wzór .....),

2) Pokój Nr – (wzór .....),

3) Pokój Nr – (wzór .....).

2. Z użyciem sprzętu komputerowego przetwarza się dane w następujących pokojach:

Nazwa zbioru (opis)	Program do przetwarzania
UG Płace	Płace INFO-SYSTEM
UG ZUS	Płatnik PROKOM Software S. A.
UG Podatki	Podatki INFO-SYSTEM
UG System Ewidencji Ludności	SEL WIN
UG Dowody osobiste	WASKO S. A.

§ 8. Wewnątrz obszaru, o którym mowa w § 7 osoby nieuprawnione do dostępu do danych osobowych mogą przebywać wyłącznie w obecności osoby zatrudnionej przy przetwarzaniu tych danych i za zgodą administratora danych lub osoby przez niego upoważnionej.

§ 9. Pomieszczenia, w których przetwarzane są dane osobowe, na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych muszą być zamykane w sposób uniemożliwiający dostęp do nich osób postronnych. Urządzenia i systemy informatyczne służące przetwarzaniu danych zasilane energią elektryczną są, przez cały czas zabezpieczone przed utratą tych danych spowodowaną awarią zasilania zakłóceniami sieci zasilającej.

§ 10. W pomieszczeniach, w których przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.

§ 11.

1. Każda osoba korzystająca z systemu informatycznego przetwarzania danych osobowych otrzymuje swój identyfikator oraz hasło.

2. Hasła oraz identyfikatory ustala administrator bezpieczeństwa informacji.

3. Hasło jest unikalne, inne dla każdej osoby, zawiera minimum pięć znaków i jest ważne przez 30 dni.

4. Identyfikatory przydzielane są jednorazowo. Osobę, która utraciła uprawnienie do dostępu do danych osobowych, niezwłocznie wyrejestrowuje się, unieważnia jej hasło oraz podejmuje inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych. Identyfikatory po wyrejestrowaniu użytkownika z systemu informatycznego nie są przydzielane innym osobom.

§ 12. Dostęp do istniejących programów zawierających dane osobowe na poszczególnych stanowiskach pracy i referatach Urzędu Gminy Kuźnica zostaje ograniczony do funkcji osoby korzystającej z danych osobowych, a wynikających z jej zakresu obowiązków.

§ 13. Osoby zatrudnione przy przetwarzaniu danych osobowych, mające do nich dostęp, obowiązane są do zachowania ich w tajemnicy (zarówno w czasie zatrudnienia, jak też po jego ustaniu).

§ 14. Użytkownicy korzystający z systemu są rejestrowani i wyrejestrowani przez administratora bezpieczeństwa informacji w rejestrze ewidencji użytkowników w systemie informatycznym poprzez podanie identyfikatora wraz z imieniem i nazwiskiem, PESEL, datą urodzenia, płcią, datą rozpoczęcia lub zakończenia pracy oraz w rejestrze ewidencji użytkowników poprzez podanie imienia i nazwiska na podstawie zakresów obowiązków przydzielanych przez Wójta Gminy.

§ 15. Użytkownicy przystępując do pracy w aplikacjach: "Płace", "Płatnik", "Podatki", "Dowody Osobiste", "Ewidencja ludności" podają nazwę użytkownika następnie hasło oraz identyfikator, zaś kończąc pracę kończą program, wyłączają komputer i drukarkę.

§ 16. System informatyczny wyposażony jest w mechanizmy uwierzytelnienia użytkownika, a także kontrolę dostępu do tych danych. Nadzór nad tym sprawuje administrator bezpieczeństwa informacji.

§ 17. Administrator bezpieczeństwa informacji tworzy kopie awaryjne, sprawdzając co tydzień, pod kątem ich dalszej przydatności, do odtworzenia danych w przypadku awarii systemu. Po ustaniu użyteczności kopii awaryjnych są one bezzwłocznie usuwane. Kopie awaryjne przechowywane są w innym pomieszczeniu niż przechowywane są zbiory danych osobowych eksploatowane na bieżąco.

§ 18. Administrator bezpieczeństwa informacji sprawdza raz w tygodniu obecność wirusów komputerowych przy użyciu odpowiedniego programu antywirusowego.

-

§ 19. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przeznaczone do:

1) **likwidacii** - pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się je w sposób uniemożliwiający ich odczytanie,

2) **przekazania innemu** podmiotowi, nie uprawnionemu do otrzymania danych osobowych pozbawia się wcześniej zapisu tych danych,

3) **naprawy** - pozbawia się przed naprawą zapisu tych danych albo naprawia sięje pod nadzorem osoby upoważnionej przez administratora danych.

§ 20. Przeglądy i konserwacje sprzętu komputerowego dokonywane są okresowo przez pracownika Urzędu pod nadzorem administratora bezpieczeństwa informacji. Konserwacje i przeglądy odbywają się przy wyłączonych komputerach tak aby zgromadzone dane nie zostały zniszczone lub odczytane przez niepowołane osoby.

§ 21. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

§ 22. Ekrany monitorów stanowisk dostępu do danych osobowych są automatycznie wyłączane po upływie pięciu minut czasu nieaktywności użytkownika, lub w przypadku urządzeń starszego typu, dokonuje się wygaszania manualnie.

§ 23. Każdej osobie, której dane są przetwarzane w systemie informatycznym, system ten zapewnia odnotowanie:

1. daty pierwszego wprowadzenia danych tej osoby,

2. źródła pochodzenia danych, jeśli dane pochodzić mogą z różnych źródeł,

3. identyfikatora użytkownika wprowadzającego dane,

4. informacji: komu, kiedy, w jakim zakresie dane zostały udostępnione, jeśli przewidziane jest udostępnianie danych innym podmiotom, chyba że dane te traktuje się jako dane powszechnie dostępne,

5. żądania czasowego lub stałego wstrzymania wykorzystania danych lub ich usunięcia, jeżeli zostały zebrane niezgodnie z prawem lub sąjuż zbędne dla celu ich zebrania.

§ 24.

1. Każdemu petentowi Urzędu Gminy Kuźnica przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do:

1) uzyskania wyczerpującej informacji, czy taki zbiór istnieje,

2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze,

3) uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące, oraz podania w powszechnie zrozumiałej formie treści tych danych,

4) uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące, chyba że administrator danych jest zobowiązany do zachowania w tym zakresie tajemnicy państwowej, służbowej lub zawodowej,

5) uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane,

6) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych,

7) czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane.

2. Osoba zainteresowana może skorzystać z prawa do informacji, o których mowa powyżej nie częściej niż raz na 6 miesięcy.

3. Na wniosek osoby, której dane dotyczą administrator danych jest obowiązany w terminie 30 dni, poinformować o przysługujących je prawach, a zwłaszcza wskazać w formie zrozumiałej odnośnie danych osobowych jej dotyczących:

1) jakie dane osobowe zawiera zbiór,

2) w jaki sposób zebrano dane,

3) w jakim celu i zakresie dane są przetwarzane,

4) w jakim zakresie oraz komu dane zostały udostępnione.

4. W razie wykazania przez osobę, której dane dotyczą, że wymagają one uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe, chyba, że dotyczy to danych, w odniesieniu do których tryb ich uzupełnienia, sprostowania lub uaktualnienia określają odrębne ustawy, administrator uzupełnia dane bez zbędnej zwłoki. W razie niedopełnienia obowiązku przez administratora, osoba której dane dotyczą, może zwrócić się do Generalnego Inspektora Ochrony Danych Osobowych z wnioskiem o nakazanie dopełnienia tego obowiązku.

5. Osoba, której dane dotyczą może wnieść pisemne, umotywowane żądanie zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację wówczas gdy przetwarzanie danych jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego. Administrator danych zaprzestaje przetwarzania kwestionowanych danych osobowycn albo bez zbędnej zwłoki przekazuje żądanie Generalnemu Inspektorowi Ochrony Danych Osobowych (GIODO), który podejmuje stosowną decyzję.

§ 25. W przypadku udostępnienia danych osobowych w celach innych niż włączenie do zbioru, administrator danych udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawnych pod warunkiem uzasadnienia w sposób wiarygodny potrzebę posiadania tych danych i że udostępnienie nie naruszy praw i wolności osób, których dane dotyczą. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej.

§ 26. Administrator danych osobowych ma obowiązek zgłoszenia GIODO zmiany obejmującej przetwarzanie nowej kategorii danych w terminie do 30 dni od dnia dokonania zmiany w zbiorze danych.

§ 27. W przypadku udostępniania danych osobowych w celach innych niż włączenie do zbioru, administrator danych, udostępnia posiadane dane osobom lub podmiotom

uprawnionym do ich otrzymania na mocy przepisów prawa zgodnie z art. 29 ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 roku Nr 101, poz. 926 z późn. zm.).

§ 28. Udostępnienie danych osobowych w celach innych niż włączenie do zbioru, następuje na pisemny wniosek.

Kuźnica, 26 września 2007 roku