

Załącznik do zarządzenia Nr 6/2007  
Wójta Gminy Krzemieniewo  
z dnia 16 sierpnia 2007 r.

**Polityka bezpieczeństwa systemów informatycznych  
Służących do przetwarzania danych osobowych  
w Urzędzie Gminy Krzemieniewo**

## SPIS TREŚCI:

Wprowadzenie .....	str. 3
Rozdział 1. Opis zdarzeń naruszających ochronę danych osobowych .....	str. 4
Rozdział 2. Zabezpieczenie danych osobowych .....	str. 5
Rozdział 3. Kontrola przestrzegania zasad zabezpieczenia danych osobowych.....	str. 6
Rozdział 4. Postępowanie przy naruszeniu ochrony danych osobowych.....	str. 6
Rozdział 5. Postanowienia końcowe.....	str. 8
Załącznik nr 1. Opis systemów informatycznych w Urzędzie Gminy Krzemieniewo .....	str. 9
Załącznik nr 2. Wzór raportu z naruszenia zasad bezpieczeństwa systemu informatycznego w Urzędzie Gminy Krzemieniewo .....	str. 12
Załącznik nr 3. Wzór wykazu osób, które zapoznały się z „Polityką bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy Krzemieniewo .....	str. 13

## WPROWADZENIE

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych w Urzędzie Gminy Krzemieniewo. 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 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”, 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 §3 rozporządzenia Prezesa Rady Ministrów z dnia 25 lutego 1999 roku w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych /Dz. U. Nr 18, poz.162/ oraz §3 i 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/.

1. „Polityka bezpieczeństwa” określa tryb postępowania w przypadku, gdy:
  - 1) stwierdzono naruszenie zabezpieczenia systemu informatycznego,
  - 2) stan urzędu, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci informatycznej mogą wskazywać na naruszenie zabezpieczeń tych danych.
2. „Polityka bezpieczeństwa” obowiązuje wszystkich pracowników Urzędu Gminy Krzemieniewo
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. Na Administratora Bezpieczeństwa Informacji wyznaczam, Sekretarza Gminy, który jest Pełnomocnikiem ds. Ochrony danych osobowych
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 Administratora danych lub osoby przez niego upoważnionej 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.

Niniejszy dokument jest zgodny z następującymi aktami prawnymi :

- 1) ustawą z dnia 29 sierpnia 1997r. O ochronie danych osobowych /Dz.U. z 2002 r. Nr 101, poz. 926 ze zmianami/,
- 2) ustawą o ochronie informacji niejawnych z dnia 22 stycznia 1999 r. /Dz.U. Nr 11, poz.95 ze zmianami/,
- 3) rozporządzeniem Prezesa Rady Ministrów z dnia 25 lutego 1999 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych /Dz.U.Nr 18, poz.162/.

## **Rozdział 1**

### **Opis zdarzeń naruszających 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 naruszona ciągłość pracy systemu, może nastąpić naruszenie poufności danych,
  - 3) zagrożenia zamierzone, świadome i celowe- najpoważniejsze zagrożenia, naruszenia poufności danych (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz(włamywanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.
2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w których przetwarzane są dane osobowe:

- 1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, np. Wybuch gazu, 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 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” ,
  - 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 2**

### **Zabezpieczenie danych osobowych**

1. Administratorem danych osobowych zawartych i przetwarzanych w systemach informatycznych Urzędu Gminy Krzemieniewo 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 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 zastosowania 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) szczególne zabezpieczenie centrum przetwarzania danych( komputer centralny, serwerownia)poprzez zastosowanie systemu kontroli dostępu,
  - 4) wyposażenie pomieszczeń w szafy dające gwarancje 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. 1 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 systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy w Krzemieniewie” 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 Gminy w Krzemieniewie i ich zabezpieczeń zawiera załącznik nr 1 do niniejszego dokumentu.

### **Rozdział 3**

#### **Kontrola przestrzegania zasad zabezpieczenia danych osobowych**

1. Administrator danych (Wójt Gminy Krzemieniewo), lub osoba przez niego wyznaczona, którą jest „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 półroczne plany kontroli zatwierdzone przez Wójta Gminy Krzemieniewo i zgodnie z nimi przeprowadza prace kontrolne oraz dokonuje kwartalnych ocen stanu bezpieczeństwa danych osobowych.
3. Na podstawie zgromadzonych materiałów, o których mowa w ust. 2, Administrator Bezpieczeństwa sporządza roczne sprawozdanie i przedstawia Administratorowi danych(Wójtowi Gminy).

### **Rozdział 4**

#### **Postępowanie w przypadku naruszenia 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 danych osobowych Administratora Bezpieczeństwa 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
4. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych Administrator Bezpieczeństwa
- 1) zapoznaje się z zaistniałą sytuacją i dokonuje metody wyboru 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 naruszeniem,
  - 3) rozważa celowość i potrzebę powiadomienia o zaistniałym naruszeniu Administratora Danych,
  - 4) nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba ze specjalistami z Urzędu.
5. Administrator Bezpieczeństwa dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg 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 postępowania naruszenia,
  - 6) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.
6. Raport, o którym mowa w ust. 5 Administrator Bezpieczeństwa niezwłocznie przekazuje Administratorowi Danych, a w przypadku jego nieobecności osobie uprawnionej.
7. 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.
8. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez kierownictwo Urzędu, Administratora Bezpieczeństwa, Pełnomocnika ds. Ochrony Informacji Niejawnych.
9. Analiza o której mowa w ust. 8, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

## **Rozdział 5**

### **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 dokumentującego 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 wg 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 nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych /Dz.U. z 2002r. Nr 101, poz. 926 ze zmianami/ 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 2002r. 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 rozporządzenia 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 sposobów zabezpieczenia danych informatycznych /Dz.U. Nr 100, poz.1023/.
6. Niniejsza „Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy w Krzemieniewie” wchodzi w życie z dniem jej podpisania przez Wójta Gminy Krzemieniewo.



**Załącznik Nr 1**

do „Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy Krzemieniewo”

**1. Wykaz pomieszczeń, w których przetwarzane są dane osobowe, opis systemów informatycznych w Urzędzie Gminy Krzemieniewo i ich zabezpieczeń.**

<b>Nr pokoju</b>	<b>Stanowisko pracy</b>	<b>System</b>
Nr 3	Stanowisko pracy ds. ewidencji i obrony	<b>ELUD</b> (ewidencja ludności)
	Kierownik USC	<b>USC</b> <b>SOO</b> (system wspomaganie wydawania dowodów osobistych)
Nr 23	Stanowisko pracy ds. ewidencji działalności gospodarczej i obrotu ziemią	<b>EPOD + SIK</b> (rejestr działalności gospodarczej)
		<b>RESP</b> (rejestr nieruchomości)
		<b>EGB</b> (ewidencja gruntów , budynków i lokali)
Nr 24	Stanowisko pracy ds. rolnictwa i gospodarki mieszkaniowej	<b>DM + SIK</b> (Dodatki mieszkaniowe)
Nr 29	Stanowisko pracy ds. księgowości budżetowej I	<b>PŁACE</b>
		<b>RP</b> (rejestr pojazdów podlegających podatkowi od środków transportu)
		<b>PŁATNIK</b> (Ewidencja – składki ZUS)
Nr 30	Stanowisko pracy ds. księgowości podatkowej I	<b>POGRUN</b> (naliczanie podatków) <b>WIP</b> (windykacja podatków i opłat)
	Stanowisko pracy ds. księgowości podatkowej II	<b>EGRUN</b> (ewidencja gruntów)

## **2. W celu ochrony przed utratą danych w Urzędzie Gminy Krzemieniewo stosowane są następujące zabezpieczenia :**

- 1) odrębna sieć energetyczna zarządzana z pomieszczenia archiwum z zabezpieczeniem przeciw burzom jak i z systemem przepięciowym, sieć trzyprzewodowa uziemniona, podzielona na obwody,
- 2) serwer i urządzenia sieciowe zasilane przez UPS EVER 600VA,
- 3) sieć komputerowa kategorii V, strukturalna, sprowadzona do pomieszczenia archiwum,
- 4) serwer z dwoma dyskami oparty na platformie LINUX,
- 5) w systemach, gdzie przetwarzane są dane osobowe, wykonuje się przynajmniej 2 razy w tygodniu kopię na płytę CD, którą przechowuje się w urzędowym sejfie,
  
- 6) dostęp do systemów znajdujących się w poszczególnych komputerach uzyskuje się po podaniu nazwy użytkownika oraz hasła (pierwszy poziom dostępu),
- 7) uzyskanie dostępu do serwera odbywa się poprzez zalogowanie: użytkownik + hasło (drugi poziom dostępu),
- 8) poszczególne programy są dodatkowo zabezpieczone poprzez podanie nazwy użytkownika oraz hasła (trzeci poziom dostępu)

## **3. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu:**

- 1) serwer ma wyłączone mechanizmy zdalnego dostępu – można na nim pracować tylko z konsoli,
- 2) na wszystkich stacjach zainstalowany jest program antywirusowy AVAST 4,7, a dodatkowo na serwerze uruchomiony jest FIREWALL,
- 3) dostęp do pomieszczenia z serwerem chroniony jest alarmem i dostęp do niego mają tylko upoważnione osoby,
- 4) wszystkie gniazdka lokalnej sieci komputerowej są galwanizowane, oddzielone od szkieletu sieci komputerowej, a podłączenie (zkrosowanie) danego użytkownika do sieci komputerowej dokonuje administrator sieci.

## **4. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu poprzez internet:**

- 1) pierwszy poziom zabezpieczenia router ASMAX BR604; zarządzanie routerem jest możliwe tylko z sieci wewnętrznej po autoryzacji i podaniu hasła,
- 2) serwer ma wyłączone mechanizmy zdalnego dostępu – można na nim pracować tylko z consoli,
- 3) na wszystkich stacjach zainstalowany jest program antywirusowy AVAST 4,7,
- 4) poczta chroniona jest przez odrębny serwer pracujący poza Urzędem,
- 5) dostęp do internetu nie jest routowany przez serwer danych .

## **5. Postanowienia końcowe.**

- 1) do pomieszczeń, w których następuje przetwarzanie danych osobowych mają dostęp tylko uprawnione osoby bezpośrednio związane z nadzorem nad serwerami lub aplikacjami,
- 2) zabezpieczenie przed nieuprawnionym dostępem do danych, prowadzone jest przez Administratora Bezpieczeństwa, zgodnie z przyjętymi procedurami nadawania uprawnień do systemu informatycznego,
- 3) osoby mające dostęp do danych powinny posiadać zaświadczenie o przebytych szkoleniu z zakresu ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz.U. Nr 133, poz. 833 ze zmianami),

- 4) w pomieszczeniach, w których zamontowany jest serwer, powinna być zamontowana klimatyzacja, która zapewnia właściwą temperaturę i wilgotność powietrza dla sprzętu komputerowego,
- 5) w pobliżu wejścia do pomieszczenia z serwerem i innymi urządzeniami, znajduje się gaśnica, która okresowo jest napełniana i kontrolowana przez specjalistę.

**Załącznik nr 2**

do „Polityki bezpieczeństwa systemów informatycznych  
służących do przetwarzania danych osobowych  
w Urzędzie Gminy Krzemieniewo”.

**Raport z naruszenia bezpieczeństwa informatycznego  
w Urzędzie Gminy Krzemieniewo.**

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 i podpis Administratora Bezpieczeństwa)

**Załącznik Nr 3**

Do „Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy Krzemieniewo

**Wykaz osób, które zostały zapoznane z „Polityką bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy Krzemieniewo”, przeznaczoną dla osób zatrudnionych przy przetwarzaniu tych danych**

Przyjęłam do wiadomości i stosowania zapisy Polityki bezpieczeństwa

<b>Imię i nazwisko</b>	<b>Stanowisko</b>	<b>Data, podpis</b>
Agata Musielak	Stanowisko pracy ds. ewidencji ludności i obrony	
Halina Dolacińska	Kierownik USC	
Krystyna Dziejic	Stanowisko pracy ds. ewidencji działalności gospodarczej i obrotu ziemią	
Ewa Stawińska	Stanowisko pracy ds. rolnictwa i gospodarki mieszkaniowej	
Gabriela Mehr	Stanowisko pracy ds. księgowości budżetowej I	
Wiesława Grybska	Stanowisko pracy ds. księgowości podatkowej I	
Maria Zygnier	Stanowisko pracy ds. księgowości podatkowej II	