

Załącznik do zarządzenia Nr 2/2012  
Wójta Gminy Krzemieniewo  
z dnia 23 stycznia 2012 r.

**POLITYKA BEZPIECZEŃSTWA I INSTRUKCJA ZARZĄDZANIA  
SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO  
PRZETWARZANIA DANYCH OSOBOWYCH  
W URZĘDZIE GMINY KRZEMIENIEWO**

Opracowała: Longina Szulc

Administrator Bezpieczeństwa Informacji

**SPIS TREŚCI:**

Wprowadzenie.....	3
Rozdział 1. Opis zdarzeń naruszających ochronę danych osobowych.....	5
Rozdział 2. Zabezpieczenie danych osobowych.....	6
Rozdział 3. Kontrola przestrzegania zasad zabezpieczenia danych osobowych.....	9
Rozdział 4. Postępowanie w przypadku naruszenia ochrony danych osobowych...9	
Rozdział 5. Monitorowanie zabezpieczeń.....	11
Rozdział 6 . Szkolenia.....	11
Rozdział 7. Niszczenie wydruków i zapisów na nośnikach magnetycznych.....	12
Rozdział 8. Archiwizacja danych.....	12
Rozdział 9. Środki ochrony oraz zasady zarządzania Zintegrowanego Modułu Obsługi Końcowego Użytkownika (ZMOKU/BUSC)	
Rozdział 10 . Postanowienia końcowe.....	12
<u>Załącznik nr 1</u> - Granice obszarów oraz osoby i wydziały , które przetwarzają dane osobowe	
<u>Załącznik nr 2</u> - Raport z naruszenia bezpieczeństwa systemu informatycznego w Urzędzie – wzór	
<u>Załącznik nr 3</u> – Szczegółowy opis środków ochrony oraz zasad zarządzania zabezpieczeniami na stanowiskach systemu teleinformatycznego ZMOKU/BUSC zlokalizowanego w Urzędzie Gminy Krzemieniewo	
<u>Załącznik nr 4</u> - Wykaz osób, które zostały zapoznane z Polityką Bezpieczeństwa.	
<u>Załącznik nr 5</u> – Oświadczenie – wzór	
<u>Załącznik nr 6</u> – Upoważnienie – wzór	
<u>Załącznik nr 7</u> – Ewidencja osób upoważnionych – wzór	

## 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 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 i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Krzemieniewo”, 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 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

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 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. Administrator danych, którym jest Wójt, swoją decyzją wyznacza Administratora Bezpieczeństwa Informacji danych zawartych w systemach informatycznych Urzędu, zwanego dalej „Administratorem Bezpieczeństwa” oraz osobę upoważnioną do zastępowania „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 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.

## 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 zakłócona 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 (włamanie 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 którym przetwarzane są dane osobowe to głównie:

- 1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak 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 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 2**

### **ZABEZPIECZENIE DANYCH OSOBOWYCH**

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

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) szczególne zabezpieczenie centrum przetwarzania danych (komputer centralny, serwerownia) poprzez zastosowanie systemu kontroli dostępu,
- 4) 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. 1, w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych,
- 1) 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 Urzędzie Gminy Krzemieniewo” 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, granice obszarów oraz osoby i Referaty, które przetwarzają dane osobowe zawiera [załącznik nr 1](#) do niniejszego dokumentu.

#### **7. 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 za pośrednictwem zasilacza awaryjnego,
- 3) sieć komputerowa kategorii V, strukturalna, sprowadzona do pomieszczenia archiwum,
- 4) serwer z dwoma dyskami (nadmiarowość RAID1) oparty na platformie Windows Server 2008,
- 5) Urządzenie NAS (nadmiarowość RAID1) pełniące rolę magazynu kopii zapasowych. Kopie są wykonywane codziennie.
- 6) uzyskanie dostępu do komputerów oraz serwera odbywa się poprzez zalogowanie: użytkownik + hasło ,
- 7) poszczególne programy są dodatkowo zabezpieczone poprzez podanie nazwy użytkownika oraz hasła

**Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu:**

- 1) W sieci jest zainstalowany router z funkcją firewalla. Dostęp zdalny jest uniemożliwiony poprzez blokowanie portów TCP i UDP.
- 2) na wszystkich stacjach zainstalowany oraz serwerze zainstalowany jest program antywirusowy Eset NOD Antivirus.
- 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 połączenie (zkrosowanie) danego użytkownika do sieci komputerowej dokonuje administrator sieci.

**Inne zabezpieczenia:**

- 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 szkoleniach 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.



## Rozdział 3

### KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Administrator danych 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 i zgodnie z nimi przeprowadza kontrole 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).

## Rozdział 4

### 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. zalenie, 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,
  - 2) 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 naruszeniem,
- 3) rozważa celowość i potrzebę powiadomienia o zaistniałym naruszeniu Administratora danych ,
- 5) nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza Urzędu.

6. 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 wystąpienia naruszenia,
- 6) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

7. Raport, o którym mowa w ust. 6, Administrator Bezpieczeństwa niezwłocznie przekazuje Administratorowi Danych (Wójtowi), a w przypadku jego nieobecności osobie uprawnionej.

8. 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.

9. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Kierownictwo urzędu, Administratora Bezpieczeństwa Informacji, Pełnomocnika ds. Ochrony Informacji Niejawnych.

10. Analiza, o której mowa w ust. 9, 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**

### **MONITOROWANIE ZABEZPIECZEŃ**

1. Prawo do monitorowania systemu zabezpieczeń posiadają , zgodnie z zakresem czynności:
  - a) Administrator Danych,
  - b) Administrator Bezpieczeństwa Informacji.
2. W ramach kontroli należy zwracać szczególną uwagę na:
  - a) okresowe sprawdzanie kopii bezpieczeństwa pod względem przydatności do możliwości odtwarzania danych,
  - b) kontrola ewidencji nośników magnetycznych,
  - c) kontrola właściwej częstotliwości zmiany hasel .

## **Rozdział 6**

### **SZKOLENIA**

1. Wszyscy pracownicy Urzędu mają obowiązek brać udział w szkoleniach ,
2. Szkolenie powinno dotyczyć:
  - a) obowiązujących przepisów i instrukcji wewnętrznych dotyczących ochrony danych osobowych, sposobu niszczenia wydruków i zapisów na nośnikach magnetycznych i optycznych,
  - b) przedstawienie zasad ochrony danych osobowych dotyczących bezpośrednio wykonywanych obowiązków na stanowisku pracy.

## **Rozdział 7**

### **NISZCZENIE WYDRUKÓW I ZAPISÓW NA NOŚNIKACH MAGNETYCZNYCH**

1. Nośniki magnetyczne przekazywane na zewnątrz powinny być pozbawione zapisów zawierających dane osobowe.,
2. Niszczenie poprzednich zapisów powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika,

3. Poprawność przygotowania nośnika magnetycznego powinna być sprawdzona przez Administratora Bezpieczeństwa Informacji,
4. Uszkodzone nośniki magnetyczne przed ich wyrzuceniem należy fizycznie zniszczyć poprzez przecięcie, przelamanie itp.
5. Wydruki po wykorzystaniu należy zniszczyć w mechanicznej niszczarce do papieru.

## **Rozdział 8**

### **ARCHIWIZACJA DANYCH**

1. Dane systemów kopiowane są w systemie codziennym.
2. Kopie awaryjne danych zapisywanych w programach wykonywane są codziennie w sposób automatyczny.
3. Odpowiedzialnym za wykonywanie kopii danych i kopii awaryjnych jest Administrator Bezpieczeństwa Informacji.
4. Na koniec danego miesiąca wykonywane są kopie bezpieczeństwa z całego programu przetwarzającego dane. Nośniki z kopiami bezpieczeństwa przechowywane są w metalowej szafie.
5. Kopie awaryjne przechowywane są w szafie metalowej - w wyznaczonym pomieszczeniu .
6. Kopie bezpieczeństwa są zapisywane na dyskach twardych i przechowywane w kasie pancerniej.
7. Płyty CD , DVD na których przechowywane byłyby kopie awaryjne niszczy się w sposób mechaniczny , tak by nie można było użyć ich ponownie,
8. Administrator Bezpieczeństwa Informacji odpowiedzialny jest za dokonywanie wymiany kopii awaryjnych na aktualne,
9. Administrator Bezpieczeństwa Informacji dokonuje okresowej weryfikacji kopii bezpieczeństwa pod kątem ich przydatności,

## **Rozdział 9**

### **ŚRODKI OCHRONY ORAZ ZASADY ZARZĄDZANIA ZINTEGROWANEGO MODUŁU OBSŁUGI KOŃCOWEGO UŻYTKOWNIKA (ZMOKU/BUSC)**

1. Szczegółowy opis środków ochrony oraz zasad zarządzania zabezpieczeniami na stanowiskach systemu teleinformatycznego ZMOKU/BUSC (dowody osobiste, ewidencja ludności, USC) zlokalizowanego w Urzędzie Gminy Krzemieniewo zawiera [Załącznik nr 3](#) do niniejszego dokumentu.

## Rozdział 10

### 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, wszczynają 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 4](#) 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 (tekst jednolity Dz. U. z 2002 r. 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 (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926), rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) oraz rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. 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 i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Krzemieniewo” wchodzi w życie z dniem jej podpisania przez Wójta.*

**Załącznik nr 1 do „ Polityki bezpieczeństwa”**

**Granice obszarów oraz osoby i wydziały , które przetwarzają dane osobowe.**

<b>POKÓJ NR 3 – parter- USC, Ewidencja Ludności, Dokumenty tożsamości</b>	
<b>Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji</b>	<b><u>Imię i nazwisko:</u></b> - Agata Musielak - Katarzyna Spychaj

<b>POKÓJ NR 6 – parter- Obrona Cywilna, Akcja Kurierska, Sprawy Wojskowe, Oświata (SIO, arkusze organizacyjne szkół, awans zawodowy nauczycieli)</b>	
<b>Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji</b>	<b><u>Imię i nazwisko:</u></b> - Zenon Rosik

<b>POKÓJ NR 9– parter – Sekretarz Gminy (Zamówienia Publiczne, Gminna Komisja Rozwiązywania Problemów Alkoholowych, ławnicy, oświadczenia majątkowe, skargi i wnioski, korespondencja i wszystkie sprawy podległe na innych stanowiskach pracy)</b>	
<b>Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji</b>	<b><u>Imię i nazwisko:</u></b> - Longina Szulc

<b>POKÓJ NR 10 – parter- Dziennik Korespondencji, Rejestr Skarg i Wniosków, oświadczenia majątkowe radnych</b>	
<b>Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji</b>	<b><u>Imię i nazwisko:</u></b> - Bogusława Stróżyńska

<b>POKÓJ NR 12 – parter- Dziennik Korespondencji, Zwrot podatku akcyzowego – producenci rolni</b>	
<b>Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji</b>	<b><u>Imię i nazwisko:</u></b> - Tomasz Stachowiak

<b>POKÓJ NR 23 – piętro- Dzierżawy wieczyste, Zezwolenia na sprzedaż napojów alkoholowych, nadawanie numerów porządkowych nieruchomościom</b>	
<b>Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji</b>	<b><u>Imię i nazwisko:</u></b> - Patrycja Skorupka

<b>POKÓJ NR 24 – piętro- Umowy na odbieranie odpadów komunalnych, Decyzje zezwalające na usunięcie drzew i krzewów, Ewidencja umów na wywóz odpadów komunalnych, Ewidencja właścicieli obiektów, w których był lub jest wykorzystywany</b>	
--	--

<b>azbest, Zamówienia publiczne</b>	
<b>Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji</b>	<b><u>Imię i nazwisko:</u></b> - Joanna Przybylska - Ewa Stawińska

<b>POKÓJ NR 27 – piętro- Decyzje o warunkach zabudowy i zagospodarowaniu terenu, Ewidencja zabytków</b>	
<b>Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji</b>	<b><u>Imię i nazwisko:</u></b> - Jerzy Dębowskiak

<b>POKÓJ NR 29– piętro- Księgowość, Kadry i płace</b>	
<b>Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji</b>	<b><u>Imię i nazwisko:</u></b> - Danuta Masztalerz - Gabriela Mehr

<b>POKÓJ NR 30– piętro- Podatki, ewidencja gruntów</b>	
<b>Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji</b>	<b><u>Imię i nazwisko:</u></b> - Wiesława Grybska - Maria Zygnier

<b>POKÓJ NR 31– piętro- Kasa</b>	
<b>Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji</b>	<b><u>Imię i nazwisko:</u></b> - Paulina Kowalik

<b>Osoby mające prawo wglądu do danych osobowych w kartotekach z uwagi na wykonywane zakresy czynności</b>	
<b>Administrator Danych</b>	<b>- Andrzej Pietrula</b>
<b>Sekretarz Gminy</b>	<b>- Longina Szulc</b>
<b>Administrator Bezpieczeństwa Informacji</b>	<b>- Longina Szulc</b>
<b>Z-ca wójta</b>	<b>- Ryszard Patelka</b>
<b>Skarbnik Gminy</b>	<b>- Dorota Andrzejewska</b>

**UWAGA!**

1. Obsługa techniczna urzędu, (**sprzątaczk** , **pracownicy gospodarczy podpisują oświadczenie** , którego wzór stanowi **załącznik nr 5** do „Polityki bezpieczeństwa”.
2. **Osoby odbywające staż, praktykę** mają wgląd do danych osobowych oraz do systemu informatycznego na podstawie **upoważnienia (zał. nr 6,7 )** nadanego przez Administratora oraz **oświadczenia (zał. nr 5 )**.



**Załącznik nr 2 do „Polityki bezpieczeństwa „ - Wzór**

**R a p o r t**  
**z naruszenia bezpieczeństwa systemu 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:

.....  
.....

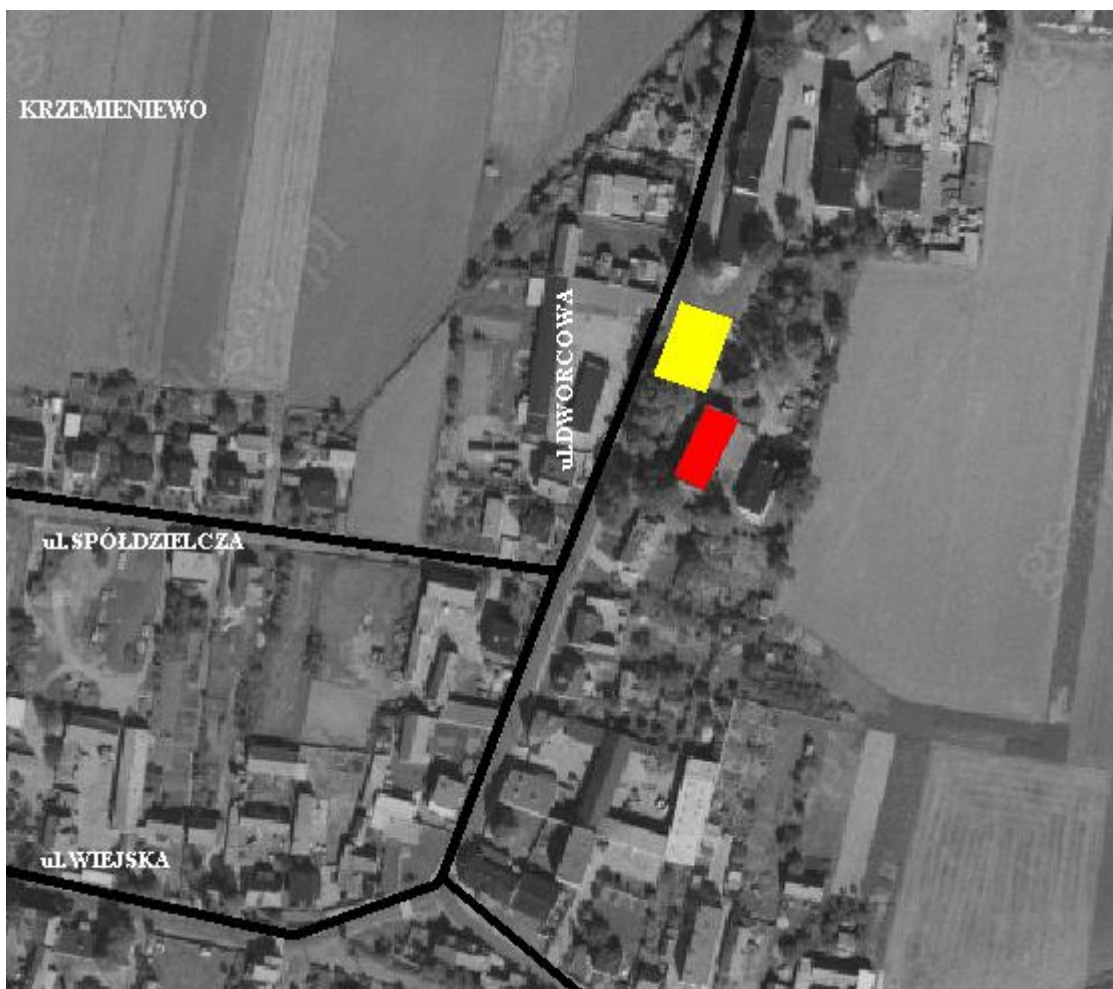
.....  
data, podpis Administratora Bezpieczeństwa Informacji

**SZCZEGÓŁOWY OPIS ŚRODKÓW OCHRONY  
ORAZ ZASAD ZARZĄDZANIA ZABEZPIECZENIAMI  
NA STANOWISKU SYSTEMU  
TELEINFORMATYCZNEGO ZMOKU/BUSC  
ZLOKALIZOWANEGO W URZĘDZIE GMINY KRZEMIENIEWO**

### 1. Budynek

Stanowisko systemu zlokalizowane jest na parterze w budynku dwukondygnacyjnym murowanym. Budynek jest siedzibą Urzędu Gminy w Krzemieniewie: 64-120 Krzemieniewo, ul. Dworcowa 34.

*MAPA ORIENTACYJNA POŁOŻENIA OBIEKTU W MIEJSCOWOŚCI*





Budynek Urzędu Gminy, w którym znajduje się serwer lokalny ZMOKU i stacja robocza



Parking

## 2. Bezpieczeństwo fizyczne

Budynek Urzędu Gminy posiada dwa wejścia. Wejście główne do budynku znajduje się od strony zachodniej, gdzie usytuowany jest parking ogólnie dostępny dla samochodów osobowych. Drugie wejście, dla pracowników znajduje się po stronie wschodniej budynku, gdzie usytuowane jest podwórze i budynek mieszkalny. Po przeciwnej stronie budynku znajduje się Niepubliczny Zakład Opieki Zdrowotnej oraz budynki mieszkalne. Od strony południowej znajduje się pawilon usługowo-handlowy, od północy budynki mieszkalne. Teren Urzędu Gminy nie jest ogrodzony.

Obszar budynku jest użytkowany przez pracowników Urzędu Gminy w Krzemieniewie, Ośrodka Doradztwa Rolniczego oraz filii Banku BPH, pracujących w trybie jednozmianowym w godzinach: poniedziałek: 8.00 - 16.00, wtorek - piątek: 7.00 - 15.00.

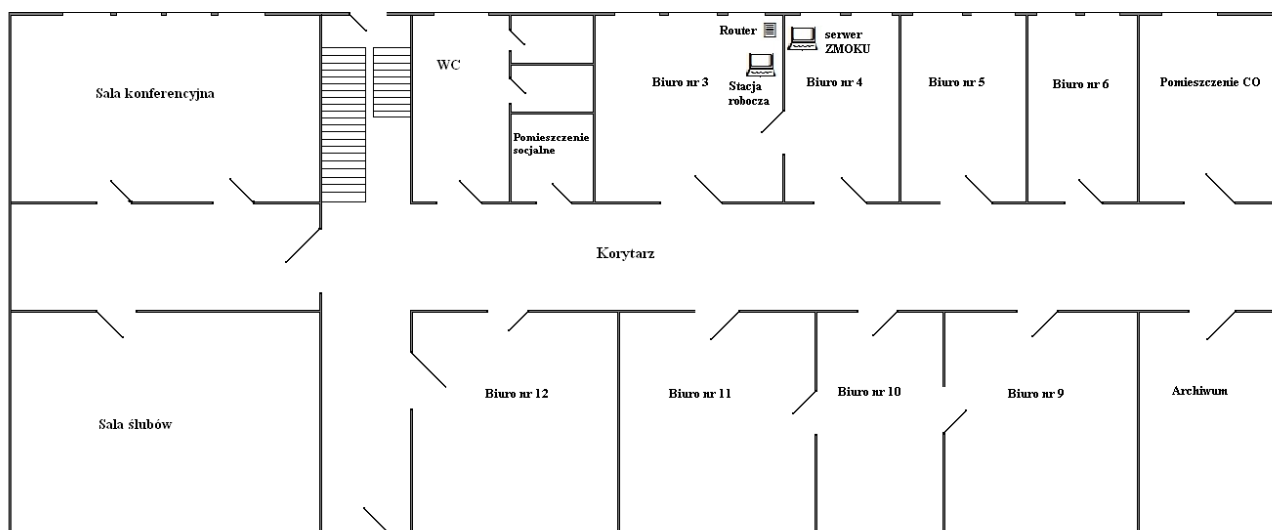
Do gmachu Urzędu Gminy w Krzemieniewie wchodzi dziennie około 120 osób (petentów i pracowników).

Do budynku urzędu wchodzi się drzwiami drewnianymi, z klamką dwustronną, zamykanymi na dwa zamki mechaniczne. Na parterze jest korytarz prowadzący na podwórze, zamykany drzwiami drewnianymi z klamką dwustronną i jednym zamkiem mechanicznym. Przy wyjściu na podwórze jest zainstalowany system włamania, detekcji ruchu.

W budynku zainstalowano system alarmowy. Urząd Gminy w Krzemieniewie posiada podpisaną umowę z firmą, która zajmuje się monitorowaniem zdarzeń włamaniowych do obiektu urzędu. Urząd jest włączony do Stacji Monitorowania Alarmów Operatora w ASC, skąd sygnał przekazywany jest do policji oraz powiadamiani są pracownicy urzędu zobowiązani do przybycia na miejsce zdarzenia.

Obszar przetwarzania danych znajduje się na parterze budynku, w strefie administracyjnej. Pomieszczenie z usytuowanym systemem IT wyposażone jest w drzwi drewniane z jednym zamkiem mechanicznym.. Pomieszczenie jest nieklimatyzowane, posiada okna z szybami antywłamaniowymi. Okna wychodzą na podwórze, na stronę wschodnią. Ściany pomieszczenia są murowane, podłoga techniczna, oświetlenie jarzeniowe. Pomieszczenie jest wyposażone w system alarmowy, detekcji ruchu. Dostęp do pomieszczenia mają tylko uprawnione osoby.

### Schemat parteru urzędu



### 3. Bezpieczeństwo elektroniczne

Router ZMOKU podpięty jest bezpośrednio do łącza internetowego. Do routera podpięta jest stacja robocza oraz serwer lokalny ZMOKU. Stacja robocza nie jest wpięta w lokalną sieć komputerową. Elementy dostarczone przez MSW zasilane są z wydzielonej sieci energetycznej wykorzystywanej również do zasilania sprzętu IT Urzędu Gminy Krzemieniewo.

### 4. Administrowanie stanowiskami

Lokalnym administratorem Systemu ZMOKU/BUSC jest Sławomir Sykała.

**Załącznik nr 4 do „Polityki bezpieczeństwa „ - Wzór**

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

Przyjąłem/am/ do wiadomości i stosowania zapisy Polityki bezpieczeństwa.

Nazwisko i Imię	Komórka organizacyjna	Data, podpis

**Załącznik nr 5 do „Polityki bezpieczeństwa” - Wzór**

.....  
/imię i nazwisko pracownika/

.....  
/adres zamieszkania/

## OŚWIADCZENIE

1. Stwierdzam własnoręcznym podpisem, że znana jest mi treść przepisów :

- a) o ochronie tajemnic prawnie chronionych stanowiących tajemnicę służbową wynikającą z Kodeksu Pracy,
- b) o ochronie danych osobowych wynikająca z ustawy o ochronie danych osobowych
- c) o odpowiedzialności karnej za naruszenie ochrony danych osobowych.

2. Zobowiązuję się nie ujawniać wiadomości, z którymi zapoznałem/am się w trakcie wykonywanych czynności służbowych .

.....  
(podpis pracownika )

.....  
(podpis złożono w obecności)

.....  
/miejsowość, data/**U P O W A Ź N I E N I E Nr.....**

Na podstawie art.37 ustawy z dnia 29 sierpnia 1999 r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.)

**U p o w a Ź n i a m**.....  
/imię i nazwisko/

zatrudnionego na stanowisku.....

do przetwarzania danych osobowych oraz do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych

W.....

/nazwa jednostki organizacyjnej/

Upoważnienie wydaje się na czas zatrudnienia w jednostce.

.....  
**Administrator Danych**

## Załącznik nr 7 do „Polityki bezpieczeństwa” - Wzór

--	--

( nazwisko i imię) (stanowisko)

L.p	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia	hasło	Uwagi
1					
2					
3					
4					

## Zakres upoważnienia:

wgląd	<b>D</b>
wprowadzanie	<b>W</b>
modyfikacja	<b>M</b>
usuwanie	<b>U</b>

(Administrator Bezpieczeństwa Informacji)

.....

(imię i nazwisko)

\_\_\_\_\_

(miejsowość, data)