Załącznik Nr 1
do Zarządzenia Nr 155/2010
Wójta Gminy Kotlin
z dnia 4 listopada 2010r.

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE GMINY KOTLIN

WPROWADZENIE

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych w Urzędzie Gminy w Kotlinie.
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.

Dokument „Polityka bezpieczeństwa w Urzędzie Gminy Kotlin" wskazuje sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych, przeznaczony jest dla osób zatrudnionych przy przetwarzaniu tych danych.

1. „Polityka bezpieczeństwa" obowiązuje wszystkich pracowników Urzędu Gminy w Kotlinie
2. Administratorem Danych jest Wójt Gminy Kotlin,
3. Administratorem Bezpieczeństwa Informacji jest wyznaczona osoba, która realizuje zadania w zakresie ochrony danych, a w szczególności:
    1) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Urzędu Gminy
    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 reagowania w przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
    4) nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nich zatrudnionych.

Rozdział 1

OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

1. Podział zagrożeń:

a) 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,

b) 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,
c) zagrożenia zamierzone, świadome i celowe – najpoważniejsze zagrożenia, naruszenia poufności danych, zagrożenia te dzielimy 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:

a) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np. wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad itp.
b) niewłaściwe parametry środowiska jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
c) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub sabotaż, a także niewłaściwe działanie serwisu,
d) pojawienie się odpowiedniego komunikatu alarmowego do tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
e) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
f) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
g) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
h) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
i) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania lub inne strzeżone elementy systemu zabezpieczeń,
j) praca w systemie lub jego sieci komputerowej wskazuje 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.,
k) ujawniono istnienie nieautoryzowanych kont dostępu do danych,
l) podmieniono lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe,
m) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji.

3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka i in.) na nośnikach tradycyjnych (papier, klisz, folia, dyskietka) w formie niezabezpieczonej.

Rozdział 2

ZABEZPIECZENIE DANYCH OSOBOWYCH

1. Administratorem danych osobowych zawartych i przetwarzanych w systemach informatycznych

Urzędu Gminy Kotlin jest Wójt.

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

   a) zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
   b) zapobiegać przed zabraniem danych przez osobę nieuprawnioną,
   c) zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.

3. Do zastosowanych środków technicznych należy:

   a) przetwarzanie danych osobowych w wydzielonych pomieszczeniach położonych w strefie administracyjnej,
   b) zabezpieczenie wejścia do pomieszczeń, o których mowa w powyżej,
   c) zabezpieczenie centrum przetwarzania danych (komputer centralny, serwerownia),
   d) wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji.

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

   a) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy przetwarzaniu danych osobowych,
   b) przeszkolenie osób o których mowa wyżej, w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych,
   c) kontrolowanie otwierania i zamykania pomieszczeń, w których są przetwarzane dane osobowe.

5. Niezależnie od niniejszych zasad opisanych w dokumencie „Polityka bezpieczeństwa w Urzędzie Gminy Kotlin" 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. W celu ochrony przed utratą danych stosowane są następujące zabezpieczenia:

   a) ochrona serwerów przed zanikiem zasilania poprzez stosowanie zasilaczy zapasowych UPS,
   b) ochrona przed utratą zgromadzonych danych przez robienie kopii zapasowych, z których w przypadku awarii odtwarzane są dane i system operacyjny,
   c) zabezpieczenia przed nieautoryzowanym dostępem do baz danych:

      - aby uzyskać dostęp do zasobów sieci, należy zwrócić się do Administratora Bezpieczeństwa Informacji z wnioskiem, w którym podane będą dane nowego użytkownika oraz zasoby jakie ma on mieć udostępnione,
      - w systemie informatycznym urzędu zastosowano podwójną autoryzację użytkownika. Pierwszej autoryzacji należy dokonać w momencie uzyskania dostępu do serwera, podając login użytkownika i hasło. Drugiej autoryzacji należy dokonać uruchamiając program użytkowy, podając login użytkownika i hasło. Dostęp do wybranej bazy danych uzyskuje się dopiero po poprawnym podwójnym zalogowaniu się do systemu informatycznego.

<u>Zabezpieczenia przed nieautoryzowanym dostępem do baz danych poprzez Internet.</u>

- w zakresie dostępu z sieci wewnętrznej Urzędu do sieci rozległej Internet zastosowano środki ochrony przed podsłuchiwaniem, penetrowaniem i atakiem z zewnątrz. Zastosowano firewall, który ma za zadanie uwierzytelnianie źródła przychodzących wiadomości oraz filtrowanie pakietów w oparciu o adres IP, numer portu i inne parametry. Ściana ogniowa składa się z bezpiecznego systemu operacyjnego i filtra pakietów. Ruch pakietów, który firewall przepuszcza jest określony przez administratora.
- Oprócz filtra pakietów (firewall) zastosowano również system wykrywający obecność wirusów w poczcie elektronicznej.

W efekcie zapewnione jest:

- zabezpieczenie sieci przed atakiem z zewnątrz poprzez blokowanie wybranych portów,
- filtrowanie pakietów i blokowanie niektórych usług,
- objęcie ochroną antywirusową wszystkich danych ściąganych z Internetu na stacjach lokalnych.

7. Postanowienia końcowe.

a) zabezpieczenie przed nieuprawnionym dostępem do danych, prowadzone jest przez Administratora Bezpieczeństwa Informacji zgodnie z przyjętymi procedurami nadawania uprawnień do systemu informatycznego.
b) w pobliżu wejścia do pomieszczenia z serwerami i innymi urządzeniami znajduje się gaśnica, która okresowo jest napełniana i kontrolowana przez specjalistę.

Rozdział 3

KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZENIA DANYCH OSOBOWYCH

1. 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 Informacji przeprowadza okresowe kontrole oraz dokonuje oceny stanu bezpieczeństwa danych osobowych.

3. Na podstawie zgromadzonych materiałów o których mowa w ust. 2, Administrator Bezpieczeństwa Informacji podejmuje stosowne działania, których celem jest właściwe i bezpieczne przetwarzanie danych osobowych w Urzędzie Gminy Kotlin.

Rozdział 4

POSTEPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. W przypadku stwierdzenia naruszenia:
   a) zabezpieczenia systemu informatycznego,
   b) technicznego stanu urządzeń,
   c) zawartości zbioru danych osobowych,
   d) ujawnienia metody pracy lub sposobu działania programu,

e) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
f) 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 Informacji

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

a) 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,
b) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
c) zaniechać, o ile to możliwe, dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
d) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
e) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
f) udokumentować wstępnie zaistniałe naruszenie,
g) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa Informacji lub osoby upoważnionej.

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

a) zapoznaje się z sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy,
b) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
c) rozważa celowość i potrzebę powiadamiania o zaistniałym naruszeniu Administratora Danych.

4. Administrator Bezpieczeństwa Informacji dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg. wzoru stanowiącego **załącznik nr 1** do Polityki Bezpieczeństwa, który powinien zawierać w szczególności:

- wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
- określenie czasu i miejsca naruszenia i powiadomienia,
- określenie okoliczności towarzyszących i rodzaju naruszenia,
- wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
- wstępną ocenę przyczyn wystąpienia naruszenia,
- ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

5. Raport, o którym mowa w pkt 4 Administrator Bezpieczeństwa Informacji niezwłocznie przekazuje Wójtowi Gminy Kotlin, a w przypadku jego nieobecności osobie uprawnionej.

6. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu Administrator Bezpieczeństwa Informacji zasięga niezbędnych opinii i proponuje (po konsultacjach ze specjalistami) 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 pracowników Urzędu Gminy Kotlin.

8. Analiza, o której mowa w pkt 7, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec naruszeniom w przyszłości.

Rozdział 5

MONITOROWANIE ZABEZPIECZEŃ

1. Prawo do monitorowania systemu zabezpieczeń posiada, zgodnie z zakresem czynności: Administrator Danych - Wójt Gminy Kotlin

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 haseł.

Rozdział 6

SZKOLENIA

1. Wszyscy pracownicy Urzędu Gminy Kotlin 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, przełamanie itp.
5. Wydruki po wykorzystaniu należy zniszczyć w mechanicznej niszczarce do papieru.

Rozdział 8

ARCHIWIZACJA DANYCH

1. Dane systemów kopiowane są w systemie miesięcznym.
2. Kopie awaryjne danych zapisywanych w programach wykonywane są codziennie.
3. Odpowiedzialnym za wykonywanie kopii danych i kopii awaryjnych jest Administrator Bezpieczeństwa Informacji.
4. Na koniec danego miesiąca wykonywane są kopie bezpieczeństwa całego programu przetwarzającego dane. Nośniki z kopiami bezpieczeństwa przechowywane są w wyznaczonym pomieszczeniu.
5. Kopie awaryjne są odpowiednio zabezpieczone w wyznaczonym pomieszczeniu.
6. Dyskietki lub inne nośniki danych na których zapisywane są kopie bezpieczeństwa są każdorazowo wymazywane i formatowane, w taki sposób, by nie można było odtworzyć ich zawartości.
7. Płyty CD, DVD na których przechowuje się 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

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 Danych zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych.

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 Informacji.

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 1997r. o ochronie danych osobowych (tekst jednolity Dz.U z 2002r. Nr 101, poz. 929) 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 1997r. o ochronie danych osobowych (tekst jednolity Dz.U. z 2002r. Nr 101,

poz. 926), rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024).

6. Niniejsza Polityka Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Gminy Kotlin obowiązuje wszystkich pracowników.

ZAŁĄCZNIK NR 1 DO POLITYKI BEZPIECZEŃSTWA

W Z Ó R

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

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)

ZAŁĄCZNIK NR 2 DO POLITYKI BEZPIECZEŃSTWA

EWIDENCJA OSÓB ZAPOZNANYCH Z POLITYKĄ BEZPIECZEŃSTWA

L.p.	Nazwisko i imię	stanowisko	Przyjąłem /am/ do wiadomości Data , podpis

ZAŁĄCZNIK NR 3 DO POLITYKI BEZPIECZEŃSTWA

U P O W A Ż N I E N I E Nr .....

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1999r. o ochronie danych osobowych (Dz.U. Nr 133, poz. 883 z późn. zm.)

U p o w a ż 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 Urzędzie Gminy w Kotlinie

Upoważnienie wydaje się na czas zatrudnienia w Urzędzie Gminy w Kotlinie

.....
/ Administrator Danych /

ZAŁĄCZNIK NR 4 DO POLITYKI BEZPIECZEŃSTWA

Wykaz zbiorów danych osobowych

NAZWA SYSTEMU																		PRACOWNIK
ELUD			FKB			POGRUN			WIP			EPOD			USC			
odczyt	zapis	modyfikacja	odczyt	zapis	modyfikacja	odczyt	zapis	modyfikacja	odczyt	zapis	modyfikacja	odczyt	zapis	modyfikacja	odczyt	zapis	modyfikacja	
X	X	X																Maria Wiła
X															X	X	X	Michał Urbaniak
			X	X	X													Irena Antczak
			X	X	X													Danuta Kasperkowiak
									X	X	X							Jolanta Jarmuż
									X	X	X							Milena Derwich
X						X	X	X	X	X	X							Lidia Mrzywka
X						X	X	X	X	X	X							Małgorzata Kucharzak
X												X	X	X				Maria Krzaczkowska

ELUD – System Ewidencji Ludności
FKB – System Finansowo-Księgowy
POGRUN, WIP – Systemy Podatkowe
EPOD – System Ewidencji Działalności Gospodarczych
USC – System Obsługi Urzędu Stanu Cywilnego