Załącznik do Zarządzenia Nr 8/2008
Burmistrza Miasta i Gminy
w Kazimierzy Wielkiej
z dnia 18 lutego 2008 r.

luty 2008 r.

SPIS TREŚCI:

WPROWADZENIE

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych funkcjonujących w Urzędzie Miasta i Gminy w Kazimierzy Wielkiej.
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 Miasta i Gminy w Kazimierzy Wielkiej", zwany dalej „Polityką bezpieczeństwa", wskazujący sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w systemach informatycznych jaki i zabezpieczenia danych przetwarzanych w formie tradycyjnej (papierowej) przeznaczony jest dla osób zatrudnionych przy przetwarzaniu tych danych.

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 Miasta i Gminy w Kazimierzy Wielkiej.

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 Kierownik jednostki, swoją decyzją wyznacza Administratora Bezpieczeństwa Informacji danych zawartych w systemach informatycznych Urzędu, zwanego dalej "Administratorem Bezpieczeństwa" oraz osobę upoważnioną do zastępowania „Administratora Bezpieczeństwa".

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

1) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych oraz zbiorach tradycyjnych 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 Osobowych 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 nich 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 r. o ochronie danych osobowych (tj. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.);

2) ustawą o ochronie informacji niejawnych z dnia 22 stycznia 1999 r. (tj. Dz. U. z 2005 r. NR 196, poz. 1631 z późn. zm.);

3) rozporządzeniem Prezesa Rady Ministrów z dnia 25 lutego 1999 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz. U. z 1999 r. Nr 18, poz. 162);

4) rozporządzeniem 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. z 2004 r. Nr 100, poz. 1024);

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, 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 Miasta i Gminy w Kazimierzy Wielkiej jest Burmistrz Miasta i 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 zabraniu 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 dokumentacj;

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 Miasta i Gminy w Kazimierzy Wielkiej" 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 Miasta i Gminy w Kazimierzy Wielkiej i ich zabezpieczeń zawiera **załącznik nr 1** do niniejszego dokumentu.

Rozdział 3

KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Administrator Danych Osobowych 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 Kierownika jednostki 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 Osobowych.

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. 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 naruszeniem;

3) rozważa celowość i potrzebę powiadamia o zaistniałym naruszeniu Administratora Danych Osobowych;

4) nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza 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 wystąpienia naruszenia;

6) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego;

6. Raport, o którym mowa w ust. 6, „Administrator Bezpieczeństwa" niezwłocznie przekazuje Administratorowi Danych Osobowych, 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 Administratora Danych Osobowych oraz Administratora Bezpieczeństwa Informacji.

9. Analiza, o której mowa w ust. 8, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie osób 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 Informacji nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) 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 r. Nr 101, poz. 926 z późn. zm.), 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. z 2004 r. Nr 100, poz. 1024) oraz rozporządzenia 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. z 2004 r. Nr 100, poz. 1023).

Załącznik nr 1
Do Polityki bezpieczeństwa systemów informatycznych
służących do przetwarzania danych osobowych

w Urzędzie Miasta i Gminy
w Kazimierzy Wielkiej

Wykaz pomieszczeń w których przetwarzane są dane osobowe, opis systemów informatycznych w Urzędzie Miasta i Gminy w Kazimierzy Wielkiej przy ul.Kościuszki 12 i ich zabezpieczeń.

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

Komórka organizacyjna	Nr pokoju	System
Wydział Administracji i Spraw Obywatelskich „Ewidencja ludności i dowody osobiste”	57	program Ewidencja Ludności szafa metalowa
Wydział Administracji i Spraw Obywatelskich Wydział Finansowy „Kadry Urzędu”	106 51	Zbiór tradycyjny – szafa metalowa program HR-Saturn
Wydział Administracji i Spraw Obywatelskich „Zbiór osób ubiegających się o podjęcie pracy w Urzędzie”	106	Zbiór tradycyjny – szafa metalowa
Wydział Administracji i Spraw Obywatelskich „Zbiór osób objętych postępowaniem przed Gminną Komisją Rozwiązywania Problemów Alkoholowych w Kazimierzy Wielkiej”	111	Zbiór tradycyjny – szafa metalowa
Urząd Stanu Cywilnego „Urząd Stanu Cywilnego w Kazimierzy Wielkiej”	2	Zbiór tradycyjny – szafa metalowa
Wydział Finansowy „Łączne zobowiązanie pieniężne, podatek od nieruchomości”	53	Zbiór tradycyjny – szafa program Łączne zobowiązanie pieniężne
Wydział Rozwoju Gospodarczego „Zbiór wniosków o przyznanie dodatków mieszkaniowych”	308	Zbiór tradycyjny – szafa program DOM
Wydział Rozwoju Gospodarczego „Zbiór wniosków osób ubiegających się o lokal z mieszkaniowego zasobu gminy”	308	Zbiór tradycyjny – szafa

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

Nazwa zbioru	Program do przetwarzania
„Ewidencja ludności i dowody osobiste”	Ewidencja Ludności
„Kadry Urzędu”	zbiór prowadzony w formie tradycyjnej – papierowej oraz przy pomocy programu HR-Saturn
„Zbiór osób ubiegających się o podjęcie pracy w Urzędzie”	zbiór prowadzony w formie tradycyjnej - papierowej
„Zbiór osób objętych postępowaniem przed Gminną Komisją Rozwiązywania Problemów Alkoholowych w Kazimierzy Wielkiej”	zbiór prowadzony w formie tradycyjnej - papierowej
„Urząd Stanu Cywilnego w Kazimierzy Wielkiej”	zbiór prowadzony w formie tradycyjnej - papierowej
„Łączne zobowiązanie pieniężne, podatek od nieruchomości”	Łączne zobowiązanie pieniężne
„Zbiór wniosków o przyznanie dodatków mieszkaniowych”	zbiór prowadzony w formie tradycyjnej – papierowej i przy pomocy programu DOM firmy WiGSoft II

„Zbiór wniosków osób ubiegających się o lokal z mieszkaniowego zasobu gminy”	zbiór prowadzony w formie tradycyjnej - papierowej

3. Wykaz struktury zbiorów danych osobowych, zakresu informacji gromadzonych w danym zbiorze i przepływu danych wewnątrz organizacji:

„Ewidencja ludności i dowody osobiste”

Dane dotyczące stałych mieszkańców:	nazwisko i imiona; nazwisko rodowe; nazwiska i imiona poprzednie; imiona i nazwiska rodowe rodziców; data i miejsce urodzenia; stan cywilny; numer aktu urodzenia i oznaczenie urzędu stanu cywilnego, który ten akt sporządził; płeć; numer PESEL; obywatelstwo (data nabycia obywatelstwa polskiego, data utraty obywatelstwa polskiego); imię i nazwisko rodowe małżonka oraz jego numer PESEL; data zawarcia związku małżeńskiego; numer aktu małżeństwa i oznaczenie urzędu stanu cywilnego, który ten akt sporządził; data rozwiązania związku małżeńskiego; sygnatura akt i oznaczenie sądu, który rozwiązał małżeństwo; data zgonu małżonka; numer aktu zgonu i oznaczenie urzędu stanu cywilnego, który ten akt sporządził; adres i data zameldowania na pobyt stały; poprzednie adresy zameldowania na pobyt stały wraz z określeniem okresu zameldowania; adres zameldowania na pobyt czasowy trwający ponad 3 miesiące wraz z określeniem okresu zameldowania; tryb wymeldowania; stopień wojskowy; nazwa, seria i numer wojskowego dokumentu osobistego oraz oznaczenie wojskowej komendy uzupełnień, w której ewidencji osoba pozostaje, lub potwierdzenie zgłoszenia się do rejestracji przedpoborowych; seria i numer aktualnego dowodu osobistego oraz serie i numery poprzednich dowodów osobistych, daty ich wydania i daty ważności oraz oznaczenie organów wydających; seria i numer karty pobytu wydanej w związku z udzieleniem zezwolenia na osiedlenie się, zezwolenia na pobyt rezydenta długoterminowego Wspólnot Europejskich, zgody na pobyt tolerowany lub nadaniem statusu uchodźcy w Rzeczypospolitej Polskiej, data jej wydania, data ważności oraz oznaczenie organu, który ją wydał; seria i numer dokumentu potwierdzającego prawo stałego pobytu, data wydania, data ważności oraz oznaczenie organu, który go wydał; seria i numer karty stałego pobytu członka rodziny obywatela Unii Europejskiej, data wydania, data ważności oraz oznaczenie organu, który ją wydał
Dane dotyczące byłych mieszkańców:	nazwisko i imiona; nazwisko rodowe; nazwiska i imiona poprzednie; imiona i nazwiska rodowe rodziców; data i miejsce urodzenia; stan cywilny; numer aktu urodzenia i oznaczenie urzędu stanu cywilnego, który ten akt sporządził; płeć; numer PESEL; obywatelstwo (data nabycia obywatelstwa polskiego, data utraty obywatelstwa polskiego); imię i nazwisko rodowe małżonka oraz jego numer PESEL; data zawarcia związku małżeńskiego; numer aktu małżeństwa i oznaczenie urzędu stanu cywilnego, który ten akt sporządził; data rozwiązania związku małżeńskiego; sygnatura akt i oznaczenie sądu, który rozwiązał małżeństwo; data zgonu małżonka; numer aktu zgonu i oznaczenie urzędu stanu cywilnego, który ten akt sporządził; adres i data zameldowania na pobyt stały; poprzednie adresy zameldowania na pobyt stały wraz z określeniem okresu zameldowania; adres zameldowania na pobyt czasowy trwający ponad 3 miesiące wraz z określeniem okresu zameldowania; tryb wymeldowania; stopień wojskowy; nazwa, seria i numer wojskowego dokumentu osobistego oraz oznaczenie wojskowej komendy uzupełnień, w której ewidencji osoba pozostaje, lub potwierdzenie zgłoszenia się do rejestracji przedpoborowych; seria i numer aktualnego dowodu osobistego oraz serie i numery poprzednich dowodów osobistych, daty ich wydania i daty

	ważności oraz oznaczenie organów wydających; seria i numer karty pobytu wydanej w związku z udzieleniem zezwolenia na osiedlenie się, zezwolenia na pobyt rezydenta długoterminowego Wspólnot Europejskich, zgody na pobyt tolerowany lub nadaniem statusu uchodźcy w Rzeczypospolitej Polskiej, data jej wydania, data ważności oraz oznaczenie organu, który ją wydał; seria i numer dokumentu potwierdzającego prawo stałego pobytu, data wydania, data ważności oraz oznaczenie organu, który go wydał; seria i numer karty stałego pobytu członka rodziny obywatela Unii Europejskiej, data wydania, data ważności oraz oznaczenie organu, który ją wydał; data wymeldowania; data zgonu oraz numer aktu zgonu i oznaczenie urzędu stanu cywilnego, który akt sporządził
Dane dotyczące obywateli polskich i cudzoziemców zameldowanych na pobyt czasowy trwający ponad 3 miesiące:	nazwisko i imiona; nazwisko rodowe; nazwiska i imiona poprzednie; imiona i nazwiska rodowe rodziców; data i miejsce urodzenia; stan cywilny; numer PESEL; obywatelstwo (data nabycia obywatelstwa polskiego, data utraty obywatelstwa polskiego); imię i nazwisko rodowe małżonka oraz jego numer PESEL; adres i data zameldowania na pobyt stały; adres zameldowania na pobyt czasowy trwający ponad 3 miesiące wraz z określeniem okresu zameldowania; stopień wojskowy; nazwa, seria i numer wojskowego dokumentu osobistego oraz oznaczenie wojskowej komendy uzupełnień, w której ewidencji osoba pozostaje, lub potwierdzenie zgłoszenia się do rejestracji przedpoborowych; seria i numer aktualnego dowodu osobistego oraz serie i numery poprzednich dowodów osobistych, daty ich wydania i daty ważności oraz oznaczenie organów wydających; seria i numer karty pobytu wydanej w związku z udzieleniem zezwolenia na osiedlenie się, zezwolenia na pobyt rezydenta długoterminowego Wspólnot Europejskich, zgody na pobyt tolerowany lub nadaniem statusu uchodźcy w Rzeczypospolitej Polskiej, data jej wydania, data ważności oraz oznaczenie organu, który ją wydał; seria i numer dokumentu potwierdzającego prawo stałego pobytu, data wydania, data ważności oraz oznaczenie organu, który go wydał; seria i numer karty stałego pobytu członka rodziny obywatela Unii Europejskiej, data wydania, data ważności oraz oznaczenie organu, który ją wydał; seria i numer karty pobytu wydanej w związku z udzieleniem zezwolenia na zamieszkanie na czas oznaczony lub zgody na pobyt tolerowany, data jej wydania, data ważności oraz oznaczenie organu, który ją wydał; data wydania, seria i numer zaświadczenia o zarejestrowaniu pobytu obywatela Unii Europejskiej oraz oznaczenie organu, który ją wydał; seria i numer karty pobytu członka rodziny obywatela Unii Europejskiej, data wydania, data ważności oraz oznaczenie organu, który ją wydał; seria i numer tymczasowego zaświadczenia tożsamości cudzoziemca, data jego wydania, data ważności oraz oznaczenie organu, który je wydał
Dane dotyczące obywateli polskich i cudzoziemców zameldowanych na pobyt czasowy trwający do 3 miesięcy:	nazwisko i imiona; data i miejsce urodzenia; adres i data zameldowania na pobyt stały; poprzednie adresy zameldowania na pobyt stały; seria i numer aktualnego dowodu osobistego oraz serie i numery poprzednich dowodów osobistych, daty ich wydania i daty ważności oraz oznaczenie organów wydających; seria i numer karty pobytu wydanej w związku z udzieleniem zezwolenia na osiedlenie się, zezwolenia na pobyt rezydenta długoterminowego Wspólnot Europejskich, zgody na pobyt tolerowany lub nadaniem statusu uchodźcy w Rzeczypospolitej Polskiej, data jej wydania, data ważności oraz oznaczenie organu, który ją wydał; seria i numer dokumentu potwierdzającego prawo stałego pobytu, data wydania, data ważności oraz oznaczenie organu, który go wydał; seria i numer karty stałego pobytu członka rodziny obywatela Unii Europejskiej, data wydania, data ważności oraz oznaczenie organu, który ją wydał; seria i numer karty pobytu wydanej w związku z udzieleniem zezwolenia na zamieszkanie na czas oznaczony lub zgody na pobyt tolerowany, data jej wydania, data ważności oraz oznaczenie organu, który ją wydał; data

	wydania, seria i numer zaświadczenia o zarejestrowaniu pobytu obywatela Unii Europejskiej oraz oznaczenie organu, który ją wydał; seria i numer karty pobytu członka rodziny obywatela Unii Europejskiej, data wydania, data ważności oraz oznaczenie organu, który ją wydał; seria i numer tymczasowego zaświadczenia tożsamości cudzoziemca, data jego wydania, data ważności oraz oznaczenie organu, który je wydał; adres pobytu czasowego oraz zamierzony czas jego trwania; data przekroczenia granicy zgłoszona przez cudzoziemca przy dopełnianiu obowiązku meldunkowego
Dane osobowe PESEL:	nazwisko i imiona; nazwisko rodowe; nazwiska i imiona poprzednie; imiona i nazwiska rodowe rodziców; data i miejsce urodzenia; stan cywilny; numer aktu urodzenia i oznaczenie urzędu stanu cywilnego, który ten akt sporządził; płeć; numer PESEL; obywatelstwo (data nabycia obywatelstwa polskiego, data utraty obywatelstwa polskiego); imię i nazwisko rodowe małżonka oraz jego numer PESEL; data zawarcia związku małżeńskiego; numer aktu małżeństwa i oznaczenie urzędu stanu cywilnego, który ten akt sporządził; data rozwiązania związku małżeńskiego; sygnatura akt i oznaczenie sądu, który rozwiązał małżeństwo; data zgonu małżonka; numer aktu zgonu i oznaczenie urzędu stanu cywilnego, który ten akt sporządził; adres i data zameldowania na pobyt stały; poprzednie adresy zameldowania na pobyt stały wraz z określeniem okresu zameldowania; adres zameldowania na pobyt czasowy trwający ponad 3 miesiące wraz z określeniem okresu zameldowania; tryb wymeldowania; stopień wojskowy; nazwa, seria i numer wojskowego dokumentu osobistego oraz oznaczenie wojskowej komendy uzupełnień, w której ewidencji osoba pozostaje, lub potwierdzenie zgłoszenia się do rejestracji przedpoborowych; seria i numer aktualnego dowodu osobistego oraz serie i numery poprzednich dowodów osobistych, daty ich wydania i daty ważności oraz oznaczenie organów wydających; seria i numer karty pobytu wydanej w związku z udzieleniem zezwolenia na osiedlenie się, zezwolenia na pobyt rezydenta długoterminowego Wspólnot Europejskich, zgody na pobyt tolerowany lub nadaniem statusu uchodźcy w Rzeczypospolitej Polskiej, data jej wydania, data ważności oraz oznaczenie organu, który ją wydał; seria i numer dokumentu potwierdzającego prawo stałego pobytu, data wydania, data ważności oraz oznaczenie organu, który go wydał; seria i numer karty stałego pobytu członka rodziny obywatela Unii Europejskiej, data wydania, data ważności oraz oznaczenie organu, który ją wydał; data zgonu oraz numer aktu zgonu i oznaczenie urzędu stanu cywilnego, który akt sporządził; seria i numer karty pobytu wydanej w związku z udzieleniem zezwolenia na zamieszkanie na czas oznaczony lub zgody na pobyt tolerowany, data jej wydania, data ważności oraz oznaczenie organu, który ją wydał; data wydania, seria i numer zaświadczenia o zarejestrowaniu pobytu obywatela Unii Europejskiej oraz oznaczenie organu, który ją wydał; seria i numer karty pobytu członka rodziny obywatela Unii Europejskiej, data wydania, data ważności oraz oznaczenie organu, który ją wydał; seria i numer tymczasowego zaświadczenia tożsamości cudzoziemca, data jego wydania, data ważności oraz oznaczenie organu, który je wydał
Ewidencja wydanych i utraconych dowodów osobistych:	nazwisko i imiona; poprzednie imiona i nazwiska; nazwisko rodowe; imiona i nazwiska rodowe rodziców; data i miejsce urodzenia; numer PESEL; wzrost; kolor oczu; płeć; fotografia i podpis osoby ubiegającej się o wydanie dowodu osobistego; adres miejsca pobytu stałego lub czasowego trwającego ponad 3 miesiące; numer i seria aktualnego i poprzednich dowodów osobistych, w tym daty ich wydania, daty ważności oraz oznaczenie organu, który je wydał

Zakres informacji gromadzonych w danym zbiorze:	Imię (imiona), nazwisko, adres, nr telefonu, NIP, numer PESEL, data urodzenia, miejsce urodzenia, imiona rodziców, nazwisko rodowe, nazwisko rodowe matki, wykształcenie, zawód, stopień naukowy, świadectwa pracy, stan cywilny, imiona dzieci i małżonka, ich daty urodzenia i numer PESEL, stosunek do powszechnego obowiązku obrony, stopień wojskowy, przynależność ewidencyjna do WKU, numer książeczki wojskowej, przydział mobilizacyjny do sił zbrojnych RP, seria i numer dowodu osobistego, znajomość języków obcych, karalność, stan zdrowia

„Zbiór osób ubiegających się o podjęcie pracy w Urzędzie"

Zakres informacji gromadzonych w danym zbiorze:	imię, nazwisko, adres, nr telefonu, data urodzenia, stan cywilny, wykształcenie, kwalifikacje, doświadczenie zawodowe

„Zbiór wniosków osób ubiegających się o lokal z mieszkaniowego zasobu gminy"

Dane osób ubiegających się o przydział mieszkania:	Nazwiska i imiona, data urodzenia, adres zamieszkania lub pobytu, PESEL, miejsce pracy, zawód, seria i numer dowodu osobistego, dochody osób tworzących gospodarstwo domowe, warunki zamieszkiwania, stan techniczny lokalu lub budynku
Dane dotyczące wszystkich osób zamieszkałych z wnioskodawcą:	imiona i nazwiska, stosunek do wnioskodawcy (członek rodziny, obcy), data zameldowania (na pobyt czasowy, stały), dochody

„Zbiór osób objętych postępowaniem przed Gminną Komisją Rozwiązywania Problemów Alkoholowych w Kazimierzy Wielkiej"

Dane dotyczące osoby, wobec której prowadzi się postępowania w sprawie skierowania na badanie przez biegłego w celu wydania opinii w przedmiocie uzależnienia od alkoholu i wskazania rodzaju zakładu leczniczego:	imię nazwisko, miejsce zamieszkania, informacje z wywiadu przeprowadzanego przez policję (stan rodzinny, stosunek do rodziny praca, nadużywanie alkoholu, zakłócanie spokoju i porządku publicznego)
Dane dotyczące rodziny:	imiona i nazwiska, stosunek pokrewieństwa, informacja o nauce/pracy

„Urząd Stanu Cywilnego w Kazimierzy Wielkiej"

Dane do aktu urodzenia:	**dane dotyczące dziecka:** nazwisko, imię (imiona), data urodzenia, miejsce urodzenia **dane dotyczące rodziców:** nazwiska, imiona, nazwiska rodowe, daty i miejsca urodzenia, miejsce zamieszkania, **dane dotyczące zgłaszającego urodzenie:** nazwisko i imię, miejsce zamieszkania
Dane do aktu małżeństwa:	**dane dotyczące osób zawierających małżeństwo:** nazwiska, imiona, nazwiska rodowe, daty i miejsca urodzenia, miejsce zamieszkania, stan cywilny **dane dotyczące rodziców:** nazwisko i imię, nazwisko rodowe **świadkowie:** nazwisko i imię
Dane do aktu zgonu:	**dane dotyczące małżonka osoby zmarłej:** nazwisko i imię, nazwisko rodowe

	dane dotyczące rodziców osoby zmarłej: imiona, nazwiska rodowe **dane dotyczące osoby zgłaszającej zgon**: nazwisko i imię, miejsce zamieszkania

„Łączne zobowiązanie pieniężne, podatek od nieruchomości"

Podatnicy podatku od nieruchomości osób fizycznych:	Imię i nazwisko, adres, nr NIP, nr REGON, rodzaj własności
Podatnicy podatku od nieruchomości osób prawnych:	-
Podatnicy podatku rolnego, leśnego:	Imię i nazwisko, adres, nr NIP, nr REGON, rodzaj własności
Podatnicy podatku od posiadania psów:	Imię i nazwisko, adres, nr NIP, nr REGON, rodzaj własności
Podatnicy podatku od środków: transportowych:	Imię i nazwisko, adres, nr NIP, nr REGON, rodzaj własności

„Zbiór wniosków o przyznanie dodatków mieszkaniowych"

Zakres informacji gromadzonych w danym zbiorze:	Nazwisko i imię, numer PESEL, data urodzenia, adres zamieszkania wnioskodawcy. Nazwisko i imię, data urodzenia, stopień pokrewieństwa członków gospodarstwa domowego wnioskodawcy. Dochody wszystkich osób tworzących gospodarstwo domowe

4. W celu ochrony przed utratą danych w Urzędzie Miasta i Gminy w Kazimierzy Wielkiej zastosowane są następujące zabezpieczenia:

1) ochrona serwerów przed zanikiem zasilania poprzez stosowanie zasilaczy zapasowych UPS.

2) ochrona przed utratą zgromadzonych danych przez robienie kopii zapasowych na płytach CD, DVD, z których w przypadku awarii odtwarzane są dane i system operacyjny.

5. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu:

1) aby uzyskać dostęp do zasobów sieci, należy zwrócić się do „Administratora Bezpieczeństwa" z odpowiednim wnioskiem w którym podane będą dane nowego 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.

6. 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 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:

1) zabezpieczenie sieci przed atakiem z zewnątrz poprzez blokowanie wybranych portów.

2) filtrowanie pakietów i blokowanie niektórych usług.

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

7. Postanowienia końcowe.

1) do pomieszczeń w których następuje przetwarzanie danych osobowych mają dostęp 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 przebytym szkoleniu z zakresu ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.).

4) w pobliżu wejścia do pomieszczenia z serwerami i innym 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 Miasta i Gminy
w Kazimierzy Wielkiej

W z ó r

R A P O R T
z naruszenia bezpieczeństwa systemu informatycznego
w Urzędzie Miasta i Gminy w Kazimierzy Wielkiej

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 3
Do Polityki bezpieczeństwa systemów informatycznych
służących do przetwarzania danych osobowych
w Urzędzie Miasta i Gminy
w Kazimierzy Wielkiej

W z ó r

Wykaz osób, które zostały zapoznane z „Polityką bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Kazimierzy Wielkiej”, przeznaczony dla osób zatrudnionych przy przetwarzaniu tych danych.

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

Nazwisko i Imię ……

Komórka organizacyjna ……

……

Data, podpis