

Zarządzenie Nr 166 /04
Burmistrza Pisu
z dnia 30 listopada 2004 r.

w sprawie ustalenia „Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Piszcu”.

Na podstawie §3 ust. 1 i 3 oraz §4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 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), zarządza się co następuje:

§ 1.

Ustala się „Politykę bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Piszcu zwaną dalej „Polityką bezpieczeństwa”, która stanowi załącznik do niniejszego zarządzenia.

§ 2.

Zobowiązuje się pracowników Urzędu Miejskiego w Piszcu do stosowania zasad określonych w „Polityce bezpieczeństwa”.

§3.

Wykonanie zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§ 4.

Zarządzenie wchodzi w życie z dniem podpisania

BURMISTRZ
Andrzej Czymborski

A. Olewnicki

Załącznik
do zarządzenia Nr 166/04
Burmistrza Pisu z dnia 30.11. 2004r.

**Polityka bezpieczeństwa systemów informatycznych
służących do przetwarzania danych osobowych
w Urzędzie Miejskim w Pisu**

Opracował: Administrator Bezpieczeństwa Informacji

listopad 2004 rok

Spis treści

Wprowadzenie.....	3
Rozdział 1. Opis zdarzeń naruszających ochronę danych osobowych.....	4
Rozdział 2. Zabezpieczenie danych osobowych.....	5
Rozdział 3. Kontrola przestrzegania zasad zabezpieczenia danych osobowych.....	6
Rozdział 4. Postępowanie przy naruszeniu ochrony danych osobowych.....	6
Rozdział 5. Postanowienia końcowe.	8

Załącznik nr 1 . Wykaz pomieszczeń w których przetwarzane są dane osobowe, opis systemów informatycznych w Urzędzie Miejskim w Pisz 9

Załącznik nr 2. Wzór raportu z naruszenia zasad bezpieczeństwa systemu informatycznego w Urzędzie. 13

Załącznik nr 3. Wzór wykazu osób które zapoznały się z „Polityką bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Pisz..... 14

WPROWADZENIE

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych w Urzędzie Miejskim w Pisz, zwanym dalej „Urzędem”

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

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

Dokument „Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie”, 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.
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 Burmistrz Pisz, 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 z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.)

- 4) nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych.
6. Osoba zastępująca Administratora Bezpieczeństwa powyższe zadania realizuje w przypadku nieobecności Administratora Bezpieczeństwa.
7. Osoba zastępująca składa Administratorowi Bezpieczeństwa relację z podejmowanych działań w czasie jego zastępstwa.
8. Niniejszy dokument jest zgodny z następującymi aktami prawnymi:
 - 1) ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.),
 - 2) ustawą z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95 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. Nr 18 poz. 162),

Rozdział 1

OPIS ZDARZEN NARUSZAJACYCH OCHRONĘ DANYCH OSOBOWYCH

1. Podział zagrożeń:

- 1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych
- 2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie 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 modyfikacją 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, regaty, 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 jest Burmistrz Pisz, zwany dalej Burmistrzem.
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 z dnia 29 sierpnia 1997 r. o ochronie danych osobowych 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,
 - 3) kontrolowanie otwierania i zamykania pomieszczeń, w których są przetwarzane dane

osobowe, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę.

5. Niezależnie od niniejszych zasad opisanych w dokumencie „Polityka bezpieczeństwa” w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informatycznych 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 Miejskiego i ich zabezpieczeń zawiera załącznik nr 1 do niniejszego dokumentu.

Rozdział 3

KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Administrator danych (Burmistrz) 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 zatwierdzane przez Burmistrza 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 (Burmistrzowi).

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 niemożności 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 powiadomienia o zaistniałym naruszeniu Administratora danych.
- 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 do „Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Pieszku”, 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. 5, Administrator Bezpieczeństwa niezwłocznie przekazuje Administratorowi danych (Burmistrzowi), 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, w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.

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

9. Analiza, o której mowa w ust. 8, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie 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 zobowiązały 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 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, 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 zabezpieczania danych informatycznych (Dz. U. Nr 100, poz. 1023).
6. Niniejsza „Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Pieszku” wchodzi w życie z dniem jej podpisania przez Burmistrza.

Wykaz pomieszczeń w których przetwarzane są dane osobowe, opis systemów informatycznych w Urzędzie Miejskim w Pieszem i ich zabezpieczeń.

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

Nr pokoju	Wydział	System
11	Wydział Gospodarki Komunalnej i Rozwoju – „Dodatki mieszkaniowe”	<u>Windows 98 SE</u>
26-27	Spraw Obywatelskich Kultury i Zdrowia – „Ewidencja Ludności”	<u>Windows 98 SE</u>
28-29	Spraw Obywatelskich Kultury i Zdrowia – „Dowody osobiste”	<u>Windows NT</u>
38	Spraw Obywatelskich Kultury i Zdrowia – „Zezwolenia na sprzedaż napojów alkoholowych”	<u>Windows 98 SE</u>
38	Spraw Obywatelskich Kultury i Zdrowia – „Ewidencja zezwoleń i licencji na wykonywanie transportu drogowego”	<u>baza danych ręczna</u>
48	Wydział Finansowy – „Ewidencja podatków od środków transportowych”	<u>Windows 95 OSR2</u>
49,50	Wydział Finansowy – „Ewidencja podatków z terenu wsi i miasta”	<u>Windows 98 SE; Windows 2000 Pro</u>
50	Wydział Finansowy – „Ewidencja podatków od nieruchomości z terenu miasta”	<u>Windows 98 SE</u>
58-59	Wydział Zagospodarowania Przestrzennego i Gospodarki Nieruchomościami – „Ewidencja Nieruchomości”	<u>baza danych ręczna</u>
59	Wydział Zagospodarowania Przestrzennego i Gospodarki Nieruchomościami – „Ewidencja czynszów, dzierżaw gruntów i opłat za użytkowanie wieczyste”	<u>MS DOS 5,22</u>
Plac Daszyńskiego 7	Urząd Stanu Cywilnego – „Księgi Stanu Cywilnego”	<u>Windows XP Pro</u>

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

Nazwa zbioru (opis)	Program do przetwarzania
„Zezwolenia na sprzedaż napojów alkoholowych”	„Alkohole”
„ Dodatki mieszkaniowe”	„Dodatki mieszkaniowe”
„ Księgi Stanu Cywilnego w Piszcu”	PB „USC”
„ Dowody osobiste”	IDL System
„ Ewidencja ludności”	„Ewidencja Ludności”
„ Ewidencja podatków z terenu wsi i miasta”	„Podatki”
„ Ewidencja podatków od środków transportowych”	„Pojazdy”
„ Ewidencja czynszów, dzierżaw gruntów i opłat za użytkowanie wieczyste”	„Czynsze”
„ Ewidencja podatków od nieruchomości z terenu miasta”	„Podatki”

3. W celu ochrony przed utratą danych w Urzędzie Miejskim w Piszcu stosowane są następujące zabezpieczenia:

- 1) odrębne zasilanie sprzętu komputerowego,
- 2) ochrona serwerów przed zanikiem zasilania poprzez stosowanie zasilaczy awaryjnych (UPS),
- 3) ochrona przed utratą zgromadzonych danych przez robienie kopii zapasowych na taśmach magnetycznych i dyskach optycznych, z których w przypadku awarii odtwarzane są dane i system operacyjny
- 4) ochrona przed awarią podsystemu dyskowego przez zastosowanie mirroringu.
Uszkodzenie jakiegokolwiek z dysków zestawu nie spowoduje utraty danych.

4. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu:

- 1) wszystkie gniazdka lokalnej sieci komputerowej są galwanicznie oddzielone od szkieletu sieci komputerowej. Podłączenia (zkrasowania) danego użytkownika do sieci komputerowej dokonuje Administrator Bezpieczeństwa.
- 2) 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.
- 3) w systemie informatycznym Urzędu zastosowano podwójną autoryzację użytkownika.. Pierwszej autoryzacji należy dokonać w momencie uzyskania dostępu do serwera Urzędu, podając login użytkownika i hasło. Drugiej autoryzacji należy dokonać uruchamiając program użytkowy, podając login użytkownika i hasło. Dostęp do wybranej bazy danych Urzędu uzyskuje się dopiero po poprawnym podwójnym zalogowaniu się do systemu informatycznego Urzędu.

5. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu poprzez Internet.

W zakresie dostępu z sieci wewnętrznej Urzędu do sieci rozległej Internet zastosowano środki ochrony przed podsłuchiwaniami, 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 bezpieczeństwa informacji.

Firewall zapisuje do logu fakt zaistnienia wyjątkowych zdarzeń i śledzi ruch pakietów przechodzących przez nią. Sieć Urzędu stanowi „czarną dziurę” dla użytkowników Internetu. Nie udostępnia się poza Lokalną Sieć Komputerową (LSK) Urzędu baz danych, aplikacji i drukarek.

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 oraz danych na serwerach
- 4) zapisywanie logów połączeń użytkowników z siecią Internet

6. Postanowienia końcowe.

- 1) do pomieszczeń w których następuje przetwarzanie danych osobowych mają dostęp tylko uprawnione osoby bezpośrednio związane z nadzorem nad serwerami lub aplikacjami.

- 2) zabezpieczenie przed nieuprawnionym dostępem do danych, prowadzone jest przez Administratora Bezpieczeństwa zgodnie z przyjętymi procedurami nadawania uprawnień do systemu informatycznego.
- 3) osoby mające dostęp do danych powinny posiadać zaświadczenie o przebytych szkoleniach z zakresu ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.).
- 4) w pomieszczeniach w których znajdują się serwery zamontowane są czujniki ruchu.
- 5) w pomieszczeniach w których znajdują się serwery powinna być zamontowana klimatyzacja, która zapewnia właściwą temperaturę i wilgotność powietrza dla sprzętu komputerowego
- 6) w pobliżu wejścia do pomieszczenia z serwerami i innymi urządzeniami znajduje się gaśnica, która okresowo jest napełniana i kontrolowana przez odpowiedniego specjalistę.

R a p o r t

z naruszenia bezpieczeństwa systemu informatycznego w Urzędzie Miejskim w Pisz

1. Data:..... Godzina:.....

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....
(Imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje))

3. Lokalizacja zdarzenia:

.....
(numer pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....
.....

5. Podjęte działania:.....

6. Przyczyny wystąpienia zdarzenia:.....

7. Postępowanie wyjaśniające:.....

data, podpis Administratora Bezpieczeństwa Informacji

Załącznik nr 3 do Polityki bezpieczeństwa
systemów informatycznych służących do
przetwarzania danych osobowych w Urzędzie
Miejskim w Pisz

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

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

[illegible]