BURMISTRZ
z Bystrzycy Kłodzkiej

Zarządzenie Nr 0151-162/2007
Burmistrza Bystrzycy Kłodzkiej
z dnia 11 czerwca 2007 r.

w sprawie wprowadzenia polityki bezpieczeństwa oraz instrukcji zarządzania system informatycznym w zakresie ochrony danych osobowych

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2001 r. Nr 142, poz. 1591 ze zm.), w związku z art. 36 ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 ze zm.) oraz § 3 - 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024) zarządzam, co następuje:

§ 1

Wprowadzić:

1. „Politykę bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Bystrzycy Kłodzkiej", w brzmieniu stanowiącym załącznik nr 1 do niniejszego zarządzenia.
2. „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Bystrzycy Kłodzkiej oraz postępowania w przypadku naruszenia zabezpieczenia systemu informatycznego", w brzmieniu określonym w załączniku nr 2 do niniejszego zarządzania.

§ 2

Zobowiązuję pracowników do zapoznania się treścią niniejszego zarządzenia, a oświadczenia o zapoznaniu dołącza się do jego akt osobowych.

§ 3

Tracą moc zarządzenia Burmistrza Bystrzycy Kłodzkiej:

1) Nr 10/99 z dnia 14 października 1999 r. w sprawie określającej sposób zrządzania systemem informatycznym w Urzędzie Miasta i Gminy w Bystrzycy Kłodzkiej,

2) Nr 11/99 z dnia 14 października 2007 r. w sprawie instrukcji określającej sposób postępowania w sytuacji naruszenia zasad ochrony danych osobowych w Urzędzie Miasta i Gminy w Bystrzycy Kłodzkiej,
3) Nr 12/99 z dnia 14 październik 1999 r. w sprawie wprowadzenia zasad postępowania przy przetwarzaniu danych osobowych w Urzędzie Miasta i Gminy w Bystrzycy Kłodzkiej.

§ 4

Nadzór nad wykonaniem zarządzenia powierzam Sekretarzowi Gminy.

§ 5

Zarządzenie wchodzi w życie z dniem podjęcia.

Burmistrz
Bystrzycy Kłodzkiej
Renata Surma

RADCA PRAWNY
11.06.2008
mgr Danuta Sinczyk

Sporządziła: H.Mielnik

Załącznik nr 1 do
Zarządzenia Burmistrza
Bystrzycy Kłodzkiej
Nr 0151- 262 / 07
z dnia 11 czerwca 2007 r.

Polityka bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Bystrzycy Kłodzkiej

Rozdział 1
Przepisy ogólne

§ 1

Celem polityki bezpieczeństwa przetwarzania danych osobowych jest zabezpieczenie przetwarzania informacji stanowiących dane osobowe w rozumieniu art. 6 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.).

§ 2

Polityka bezpieczeństwa określa:

1) wykaz budynków i pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe,
2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
3) opis struktur zbiorów danych wskazujących zawartość poszczególnych pól informatycznych i powiązań między nimi,
4) sposób przepływu danych pomiędzy poszczególnymi systemami,
5) środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzania danych osobowych.

§ 3

Przez użyte w dokumencie określenie:

1) administrator danych – rozumie się Burmistrza Bystrzycy Kłodzkiej,
2) polityka bezpieczeństwa - rozumie się politykę bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Bystrzycy Kłodzkiej,
3) urząd – rozumie się Urząd Miasta i Gminy w Bystrzycy Kłodzkiej,
4) dane osobowe – rozumie się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,

5) przetwarzanie danych osobowych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
6) zbiór danych – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym,
7) wykaz zbiorów danych – rozumie się przez to wykaz zarejestrowanych oraz nie podlegających rejestracji zbiorów danych osobowych,
8) administrator bezpieczeństwa informacji (ABI) – rozumie się wyznaczoną przez burmistrza osobę odpowiedzialną za bezpieczeństwo danych osobowych w urzędzie,
9) administrator bezpieczeństwa systemu (ABS) – osoba wyznaczona przez burmistrza, odpowiedzialna za sprawność i konserwację oraz wdrożenie technicznych zabezpieczeń systemów informatycznych w zbiorach danych osobowych przetwarzanych w urzędzie,
10) system informatyczny – rozumie się system informatyczny oraz urządzenia wchodzące w jego skład i służące do przetwarzania danych osobowych,
11) kierownik wydziału – rozumie się kierownika wydziału, w którym zatrudniony jest pracownik (użytkownik systemu informatycznego) przetwarzający dane osobowe,
12) pracownik wydziału (użytkownik systemu) – rozumie się osobę zatrudnioną w ramach stosunku pracy w urzędzie bądź osobę wykonującą określone czynności związane z przetwarzaniem danych osobowych.

§ 4

Polityka bezpieczeństwa obowiązuje wszystkich pracowników urzędu oraz osoby wykonujące w urzędzie zadania związane z przetwarzaniem danych osobowych w ramach umowy zlecenia.

§ 5

Polityka bezpieczeństwa określa środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczaniem danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Rozdział 2

Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzania danych

§ 6

Administrator danych wyznacza administratora bezpieczeństwa informacji, do którego zadań należy w szczególności:

1) realizacja przepisów ustawy o ochronie danych osobowych,
2) nadzór i kontrola systemów informatycznych służących do przetwarzania danych osobowych ,
3) nadzór nad zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe.
4) przeciwdziałanie dostępowi osób niepowołanych do pomieszczeń i systemu, w którym przetwarzane są dane osobowe,
5) przeprowadzanie kontroli w zakresie zgodności przetwarzania danych z ustawą o ochronie danych osobowych oraz stosowania niniejszej instrukcji,
6) podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,
7) informowania administratora danych lub osoby przez niego upoważnionej o przypadkach naruszenia danych osobowych.

§ 7

Administrator danych wyznacza administratora bezpieczeństwa systemu, który odpowiada za sprawność i konserwację oraz wdrożenie technicznych zabezpieczeń systemów informatycznych w zbiorach danych osobowych przetwarzanych w urzędzie, w tym w szczególności przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.

§ 8

1. Kierownik wydziału wykonuje czynności przetwarzania danych osobowych w ramach zbiorów, funkcjonujących w podległej komórce organizacyjnej, z upoważnienia administratora danych.

2. Pracownik wydziału (użytkownik systemu) dokonuje czynności przetwarzania danych osobowych, z upoważnienia administratora danych osobowych, w zakresie indywidualnych obowiązków pracowniczych bądź wskazanych czynności w umowie, z wyłączeniem czynności udostępniania danych osobowych.

§ 9

Kierownicy wydziałów poza obowiązkami wymienionymi w § 8 ust. 1 zobowiązani są do:

1) zapewnienia niezbędnych środków organizacyjno-technicznych w celu zapewnienia ochrony przetwarzania danych osobowych,
2) kontroli przestrzegania zasad i sposobu wykonywania operacji przetwarzania danych przez podległych pracowników,
3) sygnalizowania niezgodności aktów prawnych organów gminy oraz innych aktów wewnętrznych urzędu z przepisami ustawowymi w zakresie ochrony danych osobowych i przedstawiania stosownych projektów zmian, mających na celu ich dostosowanie do regulacji ustawowej,
4) zgłaszania administratorowi bezpieczeństwa informacji, planowanych przemieszczeń sprzętu komputerowego oraz dokonywania aktualizacji obszaru, w którym przetwarzane są dane osobowe,
5) nadzorowania przechowywania danych w wersji papierowej, ich archiwizowania i okresowego niszczenia oraz przechorowywania danych osobowych na dyskietkach i CD-ROM-ach.
6) sprawowania kontroli nad prawidłowym zabezpieczeniem pomieszczeń, w których są przetwarzane dane osobowe.

§ 10

1. Dostęp do danych mają wyłącznie pracownicy wyznaczeni przez administratora danych oraz osoby wykonujące w urzędzie zadania związane z przetwarzaniem danych osobowych w ramach umowy zlecenia.
2. W przypadku nowo zatrudnionych pracowników, zmiany stanowiska, zakresu obowiązku pracowniczych, bądź w sytuacji naruszenia zasad i sposobu przetwarzania danych osobowych, która ma bezpośredni wpływ na rodzaj i zakres przetwarzanych danych, kierownik wydziału zobowiązany jest bezzwłocznie skierować wniosek o wydanie bądź

cofnięcie stosownego upoważnienia oraz nadanie uprawnień do pracy, według wzoru stanowiącego załącznik nr 1 do niniejszej polityki bezpieczeństwa.

3. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych wg wzoru stanowiącego załącznik nr 2 do niniejszej polityki bezpieczeństwa.
4. Osoby upoważnione do przetwarzania danych osobowych są przed dopuszczeniem ich do tych danych zaznajamiane z obowiązującymi przepisami o ochronie danych osobowych, procedurami przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych w systemie informatycznym.
5. Każdy pracownik urzędu, zostaje poinformowany odnośnie poufności przetwarzania danych osobowych i podpisuje zobowiązanie dotyczące tajemnicy przetwarzanych danych osobowych, zarówno podczas trwania umowy o pracę (lub umowy zlecenia), jak również po jej ustaniu. Wzór oświadczenia pracownika, stanowi załącznik nr 3 do niniejszej polityki bezpieczeństwa.
6. Odpowiedzialność pracowników urzędu zatrudnionych przy przetwarzaniu danych osobowych określa ich zakres czynności.
7. Naruszenie zasad ochrony danych osobowych, w efekcie których nastąpiło udostępnienie danych osobie nieupoważnionej, jest ciężkim naruszeniem obowiązków pracowniczych.
8. Ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzi Wydział Organizacyjno – Prawny.

§ 11

Osoby wymienione w § 8 ust. 2 są zobowiązane do:

1) zapoznania się z przepisami prawa w zakresie ochrony danych osobowych,
2) stosowania określonych przez administratora danych osobowych zasad, procedur oraz wytycznych mających na celu właściwe i adekwatne przetwarzanie danych,
3) należytego zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym,
4) zachowania szczególnej staranności w trakcie dokonywania operacji przetwarzania danych w celu ochrony interesów osób, których dane dotyczą,
5) podporządkowania się poleceniom kierownika wydziału i przestrzegania ustalonych przez niego szczegółowych zasad i procedur związanych z przestrzeganiem danych osobowych.

§ 12

1. Budynek urzędu, w którym zlokalizowany jest obszar przetwarzania danych osobowych jest zamykany po zakończeniu pracy oraz zabezpieczony alarmem.
2. Obszarem przetwarzania danych osobowych są pomieszczenia lub części pomieszczeń w budynku Urzędu Miasta i Gminy w Bystrzycy Kłodzkiej przy ul. H. Sienkiewicza 6 oraz pomieszczenia w budynku Ratusza pl. Wolności 1, w których przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego lub w formie papierowej.
3. Wykaz budynków, pomieszczeń lub części pomieszczeń urzędu, o których mowa w ust. 2 stanowi załącznik nr 4 do niniejszej polityki bezpieczenstwa.
4. Pomieszczenia, w których są przetwarzane dane osobowe powinny być zamykane na czas nieobecności w nich osób zatrudnionych.
5. Przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych jest tylko w obecności osoby zatrudnionej przy przetwarzaniu danych.
6. W przypadku przebywania osób postronnych w pomieszczeniach, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.
7. Wydruki oraz inne dokumenty przeznaczone do likwidacji muszą być trwale uszkodzone w sposób uniemożliwiający odczytanie z nich informacji osobowych.
8. Urządzenia lub nośniki informatyczne zawierające dane osobowe przeznaczone do przekazania innemu podmiotowi, pozbawia się wcześniej zapisu tych danych.

§ 13

1. Sposób zarządzania systemem informatycznym w urzędzie w zakresie przetwarzania danych osobowych określa odrębna instrukcja.
2. Kartoteki papierowe oraz wydruki zawierające dane osobowe znajdują się w szafach, zamykanych na zamki w pokojach, w których przetwarzane są dane osobowe.
3. Postępowanie w sytuacji naruszenia ochrony danych osobowych w systemie informatycznym określono w rozdziale 7 instrukcji, o której mowa w ust. 1.
4. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia pomieszczeń oraz miejsc przechowywania danych osobowych w formie papierowej, na dyskietkach itp.

§ 14

W przypadku konieczności utworzenia nowego zbioru danych, wynikającej z obowiązków nałożonych przepisami ustawy bądź nowymi zadaniami, kierownik wydziału zobowiązany jest niezwłocznie – nie później jednak niż w ciągu 30 dni od dnia powstania obowiązku utworzenia zbioru– zgłosić wniosek o dokonanie rejestracji zbioru danych zgodnie z obowiązującymi w tym zakresie przepisami.

§ 15

1. W obiegu zewnętrznym dane osobowe udostępnia się ze zbiorów zgodnie z powszechnie obowiązującymi w tym zakresie przepisami.
2. W obiegu wewnętrznym między komórkami organizacyjnymi urzędu, chyba że przepisy szczególne stanowią inaczej, można udostępniać dane osobowe w następującym trybie: informacje zawierające dane : imię, nazwisko, adres zamieszkania i inne o charakterze podstawowym, bezpośrednio identyfikujące osobę fizyczną może udostępnić pracownik przetwarzający dane w formie bezpośredniej lub telefonicznej, po sprawdzeniu tożsamości w procedurze „zwrotnej informacji telefonicznej.
3. Przekazywanie danych w trybie ust.2, może odbywać się tylko i wyłącznie w przypadku toczącego się postępowania administracyjnego bądź cywilnego w stosunku do osoby, której dane dotyczą.
4. W obiegu zewnętrznym zgodę na udostępnienie danych osobowych wyraża administrator danych zgodnie z obowiązującymi w tym zakresie przepisami.

§ 16

1. W umowach zawieranych przez komórki organizacyjne urzędu, w przypadku zaistnienia okoliczności powierzenia danych osobowych podmiotowi zewnętrznemu w celu wykonania określonych czynności na tych danych, każdorazowo wymagany jest zapis o powierzeniu danych osobowych bądź zawarcie odrębnej umowy powierzenia.
2. W przypadkach, o których mowa w ust.1,właściwy kierownik wydziału niezwłocznie, nie później jednak niż w ciągu 15 dni:
   1) przed podpisaniem umowy, w której został zawarty zapis o powierzeniu,
   2) przed datą planowanego powierzenia danych, na podstawie odrębnej umowy powierzenia

   przekazuje administratorowi bezpieczeństwa informacji projekt stosownej umowy.

§ 17

1. Administrator bezpieczeństwa informacji przeprowadza co najmniej raz do roku audyt, celem dokonania oceny stanu bezpieczeństwa przetwarzania danych osobowych.
2. Z audytu, o którym mowa w ust. 1 sporządza się raport wg wzoru stanowiącego załącznik nr 5 do niniejszej polityki bezpieczeństwa, który przedkłada się administratorowi danych.

Rozdział 3

Zbiory danych osobowych, opis ich struktur oraz zastosowanych programów do przetwarzania tych danych

§ 18

1. Wykaz zbiorów danych osobowych w urzędzie wraz ze wskazaniem programów zastosowanych do przetwarzania danych osobowych określa załącznik nr 6 do niniejszej polityki bezpieczeństwa.
2. Opis struktury zbiorów danych osobowych wskazujący zawartość poszczególnych pól informatycznych określa załącznik nr 7 do niniejszej polityki bezpieczeństwa.

§ 29

W urzędzie występuje następujący przepływ danych pomiędzy poszczególnymi systemami informatycznymi w sieci lokalnej:

System KADRY - istnieje możliwość przepływu danych osobowych z systemu ELUD+. Jest możliwość tylko odczytu tych danych, czyli ruch jest jednokierunkowy. Istnieje mechanizm sprawdzający przy wybraniu konkretnej osoby czy dane osobowe nie uległy zmianie. System w przypadku zauważenia zmian zadaje pytanie czy zaktualizować dane. Wybór należy do użytkownika systemu z uprawnieniami do zapisu w danym systemie.

System PŁACE - istnieje możliwość przepływu danych osobowych z systemu ELUD+ oraz z systemu KADRY. Jest możliwość tylko odczytu tych danych, czyli ruch jest jednokierunkowy. Istnieje mechanizm sprawdzający przy wybraniu konkretnej osoby czy dane osobowe nie uległy zmianie. System w przypadku zauważenia zmian zadaje pytanie czy zaktualizować dane. Wybór należy do użytkownika systemu z uprawnieniami do zapisu w danym systemie.

Eksportowane są dane w postaci pliku, o formacie ustalonym przez twórców programu PŁATNIK. Plik ten jest importowany przez system PŁATNIK, który służy do rozliczeń pracowników z ZUS. Transmisja danych do ZUS odbywa się przez teletransmisję, drogą jaką określił ZUS

System EPOD - - istnieje możliwość przepływu danych osobowych z systemu ELUD+. Jest możliwość tylko odczytu tych danych, czyli ruch jest jednokierunkowy. Istnieje mechanizm sprawdzający przy wybraniu konkretnej osoby czy dane osobowe nie uległy zmianie. System w przypadku zauważenia zmian zadaje pytanie czy zaktualizować dane. Wybór należy do użytkownika systemu z uprawnieniami do zapisu w danym systemie.

System POGRUN+ - istnieje możliwość przepływu danych osobowych z systemu ELUD+. Jest możliwość tylko odczytu tych danych, czyli ruch jest jednokierunkowy. Istnieje mechanizm sprawdzający przy wybraniu konkretnej osoby czy dane osobowe nie uległy zmianie. System w przypadku zauważenia zmian zadaje pytanie czy zaktualizować dane. Wybór należy do użytkownika systemu z uprawnieniami do zapisu w danym systemie.

System KASA+ - istnieje możliwość przepływu danych osobowych z systemu ELUD+. Jest możliwość tylko odczytu tych danych, czyli ruch jest jednokierunkowy. Istnieje mechanizm sprawdzający przy wybraniu konkretnej osoby czy dane osobowe nie uległy zmianie. System w przypadku zauważenia zmian zadaje pytanie czy zaktualizować dane. Wybór należy do użytkownika systemu z uprawnieniami do zapisu w danym systemie.

System STM - - istnieje możliwość przepływu danych osobowych z systemu ELUD+. Jest możliwość tylko odczytu tych danych, czyli ruch jest jednokierunkowy. Istnieje mechanizm sprawdzający przy wybraniu konkretnej osoby czy dane osobowe nie uległy zmianie. System w przypadku zauważenia zmian zadaje pytanie czy zaktualizować dane. Wybór należy do użytkownika systemu z uprawnieniami do zapisu w danym systemie.

System WIP+ - istnieje możliwość przepływu danych osobowych z systemu ELUD+. Jest możliwość tylko odczytu tych danych, czyli ruch jest jednokierunkowy. Istnieje mechanizm sprawdzający przy wybraniu konkretnej osoby czy dane osobowe nie uległy zmianie. System w przypadku zauważenia zmian zadaje pytanie czy zaktualizować dane. Wybór należy do użytkownika systemu z uprawnieniami do zapisu w danym systemie. Istnieje mechanizm importu

danych z systemu POGRUN+ ,KASA+ ,STM - chodzi tutaj o przypisy lub odpisy podatkowe, wpłaty i wypłaty gotówki oraz informacje o mandatach wystawionych przez Straż miejską. Dane te są zapisywane na kontach podatników.

Załącznik nr 1 do polityki
bezpieczeństwa stanowiącej załącznik nr 1 do
zarządzenia Burmistrza Bystrzycy Kłodzkiej
Nr 0151-262/07.z dnia 11 czerwca 2007 r.

W N I O S E K

W związku z *):
1) zmianą stanowiska .....

2) zmianą zakresu obowiązków .....

3) utworzeniem nowego zbioru danych osobowych .....

4) naruszeniem zasad i sposobu przetwarzania danych osobowych

*) właściwe zakreślić i wypełnić

w n i o s k u j ę

o wydanie upoważnienia/ o cofnięcie upoważnienia *)

wydanego w dniu .....

Pani/ Panu .....

zatrudnionemu na stanowisku .....

w Wydziale .....

do przetwarzania danych osobowych wynikających z zakresu obowiązków pracowniczych, z wyłączeniem udostępniania danych osobowych oraz nadania (zmianę) uprawnień do pracy w systemie informatycznym Urzędu Miasta i Gminy w Bystrzycy Kłodzkiej.

Bystrzyca Kłodzka, dnia.....

.....
(podpis wnioskodawcy)

*) niewłaściwe zakreślić

Załącznik nr 2 do polityki
bezpieczeństwa stanowiącej załącznik nr 1do
zarządzenia Burmistrza Bystrzycy Kłodzkiej
Nr 0151-262/07.z dnia 11 czerwca 2007 r.

Bystrzyca Kłodzka, dnia .....

Or...../.....

U P O W A Ż N I E N I E

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz.926 ze zm.)

u p o w a ż n i a m

Panią/ Pana .....

Stanowisko .....

Wydział .....

.....

do przetwarzania danych osobowych na podstawie przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2002 Nr 101, poz.926 ze zm.), rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024) oraz wydanych w tym zakresie zarządzeń burmistrza.

Upoważnienie niniejsze nie upoważnia do udzielania dalszych upoważnień i jest ważne na okres zatrudnienia w Urzędzie Miasta i Gminy w Bystrzycy Kłodzkiej przy przetwarzaniu danych osobowych.

Upoważnienie może być w każdym czasie odwołane.

.....

(podpis)

Załącznik nr 3 do polityki
bezpieczeństwa stanowiącej załącznik do
zarządzenia Burmistrza Bystrzycy Kłodzkiej
Nr 0151-262/07.z dnia 11 czerwca 2007 r.

.....
Imię i nazwisko składającego
oświadczenie

OŚWIADCZENIE

Ja niżej podpisany/a ..... oświadczam, że zaznajomiłem/am się z przepisami dotyczącymi ochrony danych osobowych*) i zobowiązuję się do przestrzegania tajemnicy dotyczącej ochrony danych osobowych, do których mam lub będę miał/a dostęp w związku z wykonywaniem obowiązków służbowych w trakcie okresu mojego zatrudnienia w Urzędzie Miasta i Gminy w Bystrzycy Kłodzkiej, jak i po jego ustaniu.

Przyjmuję również do wiadomości, że nie przestrzeganie w/w przepisów uznane może zostać za naruszenie obowiązków pracowniczych i wyciągnięte mogą zostać wobec mnie konsekwencje prawne.

....

(miejsce i data złożenia oświadczenia) (czytelny podpis składającego oświadczenie)

*)

1) ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. Z 2002 r. Nr 101, poz. 926 ze zm.),
2) rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024)
3) zarządzenie Burmistrza Bystrzycy Kłodzkiej Nr 0151-262/07 z dnia 11 czerwca 2007 r. w wprowadzenia polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym w zakresie ochrony danych osobowych.

Załącznik nr 4 do polityki
bezpieczeństwa stanowiącej załącznik do
zarządzenia Bystrzycy Kłodzkiej
Nr 0151-262/07.z dnia 11 czerwca 2007 r.

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są zbiory danych osobowych

Lp.	Nazwa zbiorów danych osobowych	Pomieszczenia, w których przetwarzane są zbiory danych osobowych	Stanowisko przetwarzające zbiory danych osobowych
Dane osobowe przetwarzane w budynku Urzędu Miasta i Gminy w Bystrzycy Kłodzkiej, ul. Sienkiewicza 6			
1.	Ewidencja ludności i dowodów osobistych	23-26	Stanowiska ds. ewidencji ludności i dowodów osobistych
2.	Urząd Stanu Cywilnego	72	Kierownik Urzędu Stanu Cywilnego Stanowiska ds. akt urzędu stanu cywilnego
3.	Windykacja podatków	45	Stanowiska ds. windykacji podatków
4.	Wymiar podatkowy	31-32	Stanowiska ds. wymiaru podatków
5.	Ewidencja gruntów	17-20	Stanowisko ds. ewidencji gruntów
6.	Ewidencja działalności gospodarczej	13	Kierownik Wydziału Przedsiębiorczości i Rozwoju Lokalnego
7.	Ewidencja działalności gospodarczej	14	Stanowisko ds. ewidencji działalności gospodarczej
8.	Rejestr zezwoleń na sprzedaż alkoholu	13	Kierownik Wydziału Przedsiębiorczości i Rozwoju Lokalnego
9.	Rejestr zezwoleń na sprzedaż alkoholu	14	Stanowisko ds. rejestru zezwoleń na sprzedaż alkoholu
10.	Rejestr poborowych	15	Kierownik Wydziału Spraw Obywatelskich
11.	Rejestr osób o nieuregulowanym stosunku do służby wojskowej	15	Kierownik Wydziału Spraw Obywatelskich
12.	Rejestr przedpoborowych	15	Kierownik Wydziału Spraw Obywatelskich
13.	Kadry	6	Stanowisko ds. kadr

Załącznik nr 5 do polityki
bezpieczeństwa stanowiącej załącznik nr 1 do
zarządzenia Burmistrza Bystrzycy Kłodzkiej
Nr 0151-262/07.z dnia 11 czerwca 2007 r.

RAPORT

z audytu bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Bystrzycy Kłodzkiej

Data .....

Wydziały/ samodzielne stanowiska .....

.....

.....

.....

Opis stwierdzonych nieprawidłowości w zakresie przetwarzania danych osobowych :.....

.....

.....

.....

.....

Przyczyny wystąpienia nieprawidłowości .....

.....

.....

Zalecenia i wytyczne z audytu: .....

.....

.....

.....

.....

(data i podpis administratora
bezpieczeństwa informacji)

Załącznik nr 6 do polityki
bezpieczeństwa stanowiącej załącznik do
zarządzenia Bystrzycy Kłodzkiej
Nr 0151-262/07.z dnia 11 czerwca 2007 r.

Wykaz zbiorów danych osobowych ze wskazaniem programów zastosowanych do przetwarzania danych osobowych

Lp.	Nazwa zbioru danych osobowych	Nazwa programu zastosowanego do przetwarzania danych osobowych	Autor programu
1.	Ewidencja ludności i dowodów osobistych	ELUD	Systemy komputerowe RADIX, Gdańsk ul. Piastowska 33
2.	Urząd Stanu Cywilnego	NOVELL	P.T.H. Technika sp. z o.o. Ul. Toszecka 2 44-102 Gliwice
3	Windykacja podatków	WIP	Systemy komputerowe RADIX, Gdańsk ul. Piastowska 33
4.	Wymiar podatkowy	POGRUN	Systemy komputerowe RADIX, Gdańsk ul. Piastowska 33
5.	Ewidencja gruntów	EGW	Systemy komputerowe RADIX, Gdańsk ul. Piastowska 33
6.	Ewidencja działalności gospodarczej	EPOD	Systemy komputerowe RADIX, Gdańsk ul. Piastowska 33
7.	Rejestr zezwoleń na sprzedaż alkoholu	Koncesje alkoholowe	SPUTNIK SOFTWARE Sp. z o.o. ul. Kordeckiego 30b 60-144 Poznań
8.	Kadry	KADRY	Systemy komputerowe RADIX, Gdańsk ul. Piastowska 33

Załącznik nr 7 do polityki
bezpieczeństwa stanowiącej załącznik do
zarządzenia Bystrzycy Kłodzkiej
Nr 0151-262/07.z dnia 11 czerwca 2007 r.

Opis struktury zbiorów danych osobowych wskazujący zawartość poszczególnych pól informatycznych

Lp.	Nazwa zbioru danych osobowych	Opis struktury zbiorów danych osobowych
1.	Ewidencja ludności i dowodów osobistych	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce zamieszkania lub pobytu, miejsce urodzenia, numer ewidencyjny PESEL, seria i numer dowodu osobistego oraz jego wystawca, seria i numer paszportu obcokrajowca, obywatelstwo, numer karty stałego pobytu, płeć, nazwisko rodowe, poprzednie nazwiska, nazwiska rodowe rodziców, numery ewidencyjne rodziców, numer aktu urodzenia i jego wystawca, stan cywilny, numer ewidencyjny współmałżonka, data i numer aktu małżeństwa oraz jego wystawca, poprzednie adresy zameldowania, data zgonu i numer aktu zgonu oraz jego wystawca, zmiany dotyczące wszystkich wymienionych danych osobowych (z podaniem daty i podstawy zmiany), obowiązek wojskowy, stopień wojskowy, nazwa i numer wojskowego dokumentu osobistego i jego wystawca.
2.	Urząd Stanu Cywilnego	Nazwiska i imiona, imiona rodziców, data urodzenia, nazwiska rodowe, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, wykształcenie, seria i numer dowodu osobistego lub paszportu, poprzednie nazwiska, nazwisko rodowe, źródło utrzymania, narodowość, zaświadczenie o zdolności prawnej z innych krajów, wyroki i postanowienia sądowe, decyzje z innych USC, data i numer aktu urodzenia oraz jego wystawca, data i numer aktu małżeństwa oraz jego wystawca, data i numer aktu zgonu oraz jego wystawca, nazwiska rodziców, imię i nazwisko współmałżonka, płeć, stan cywilny, data i miejsce zawarcia małżeństwa
3.	Windykacja podatków	Nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, numer identyfikacji podatkowej NIP
4.	Wymiar podatkowy	Nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, sposoby władania, adresy gospodarstw i nieruchomości, numer identyfikacji podatkowej NIP

5.	Ewidencja gruntów	Nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, numery ksiąg wieczystych, sposoby władania
6.	Ewidencja działalności gospodarczej	Nazwiska i imiona, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, adresy prowadzonej działalności gospodarczej, nazwiska i imiona oraz adresy zamieszkania pełnomocników
7.	Kadry	Nazwiska i imiona, imiona rodziców, data urodzenia, płeć, nazwisko rodowe, miejsce urodzenia, adres zamieszkania lub pobytu, seria i nr dowodu osobistego, numer ewidencyjny PESEL, numer identyfikacji podatkowej NIP, stan cywilny, stosunek do służby wojskowej, seria i numer książeczki wojskowej, wykształcenie, zawód, kwalifikacje, stanowisko, poprzednie miejsce pracy, numer telefonu, numer fax-u, kod tytułu ubezpieczenia, kod Kasy Chorych, kod wykonywanego zawodu, stopień niepełnosprawności, nazwiska i imiona dzieci, numery ewidencyjne PESEL i numery NIP dzieci oraz ich data urodzenia.
7.	Rejestr zezwoleń na sprzedaż alkoholu	Nazwisko i imię, adres punktu sprzedaży, adres zamieszkania, numer ewidencyjny PESEL, numer identyfikacji podatkowej NIP.
8,	Rejestr poborowych	Nazwisko i imię, imię ojca, data urodzenia, seria i nr dowodu osobistego, miejsce aktualnego pobytu stałego, czasowego ponad 2 miesiące, seria i numer książeczki wojskowej, nazwa WKU wdającej książeczkę wojskową, numer ewidencyjny PESEL, data zgłoszenia się do poboru, kategoria zdrowia, przyczyny nie zgłoszenia się do poboru (pobyt w areszcie, zakładzie karnym, szpitalu).
9.	Rejestr osób o nieuregulowanym stosunku do służby wojskowej	Nazwisko i imiona, imię ojca, data urodzenia, adres zamieszkania lub pobytu, informacje o pobycie w aresztach, zakładach karnych, szpitalach, data zgłoszenia się do poboru, seria i numer książeczki wojskowej, kategoria zdrowia.
10.	Rejestr przedpoborowych	Nazwisko i imiona, imię ojca, data urodzenia, adres zamieszkania lub pobytu, informacje o pobycie w aresztach, zakładach karnych, szpitalach, data zgłoszenia się do poboru, seria i numer książeczki wojskowej, kategoria zdrowia, data zgłoszenia się do rejestracji, nr potwierdzenia zgłoszenia się do rejestracji.

Załącznik nr 2 do
Zarządzenia Burmistrza
Bystrzycy Kłodzkiej
Nr 0151- 262 / 07
z dnia 1 czerwca 2007 r.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Bystrzycy Kłodzkiej

Rozdział 1
Przepisy ogólne

§ 1

Instrukcja określa ogólne zasady zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Bystrzycy Kłodzkiej.

§ 2

Przez użyte w instrukcji określenie:

1) administrator danych – rozumie się Burmistrza Bystrzycy Kłodzkiej,
2) urząd – rozumie się Urząd Miasta i Gminy w Bystrzycy Kłodzkiej,
3) dane osobowe – rozumie się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
4) przetwarzanie danych osobowych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
5) administrator bezpieczeństwa informacji (ABI) – rozumie się wyznaczoną przez burmistrza osobę odpowiedzialną za bezpieczeństwo danych osobowych w urzędzie,
6) administrator bezpieczeństwa systemu (ABS) – osoba wyznaczona przez burmistrza, odpowiedzialna za sprawność i konserwację oraz wdrożenie technicznych zabezpieczeń systemów informatycznych w zbiorach danych osobowych przetwarzanych w urzędzie,

7) system informatyczny – rozumie się system informatyczny oraz urządzenia wchodzące w jego skład i służące do przetwarzania danych osobowych,
8) zabezpieczenie systemu informatycznego –rozumie się zespół zastosowanych środków technicznych i fizycznych w celu zabezpieczenia danych osobowych przed ujawnianiem, zniszczeniem, utratą, a także nieuprawnionym dostępem lub modyfikacją,
9) kierownik wydziału – rozumie się kierownika wydziału, w którym zatrudniony jest pracownik (użytkownik systemu informatycznego) przetwarzający dane osobowe,
10) pracownik wydziału (użytkownik systemu) – rozumie się osobę zatrudnioną w ramach stosunku pracy w urzędzie bądź osobę wykonującą określone czynności związane z przetwarzaniem danych osobowych w systemie informatycznym,
11) ustawa o ochronie danych osobowych – rozumie się ustawę z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. z 2001 r. Nr 101, poz. 926 z późn. zm.),
12) rozporządzenie – rozumie się rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024).

§ 3

Przetwarzanie danych osobowych w systemie informatycznym może odbywać się zgodnie z zobowiązującą ustawą o ochronie danych osobowych, wydanych na jej podstawie aktów wykonawczych oraz niniejszej instrukcji.

§ 4

Osobą odpowiedzialną za bezpieczeństwo danych osobowych w systemach informatycznych przetwarzających dane osobowe jest administrator bezpieczeństwa systemu.

§ 5

Przetwarzanie danych osobowych jest możliwe tylko przez uprawnione osoby w wyznaczonym przez administratora danych obszarze podlegającym szczegółowej ochronie i zabezpieczeniu.

§ 6

Szczegółowe wdrożenie programowych i sprzętowych rozwiązań w zakresie zabezpieczenia danych osobowych zapewnia administrator bezpieczeństwa systemu.

§ 7

W urzędzie funkcjonują następujące systemy informatyczne:

1) EGRUN+ - System Ewidencji Mienia Komunalnego EGRUN służy do prowadzenia ewidencji gruntów i budynków w układzie rejestru gruntów i budynków dostosowanym do aktualnie obowiązujących przepisów, prowadzenia pełnej ewidencji mienia komunalnego, archiwizacji jednostek rejestrowych oraz sporządzania zestawień ewidencji gruntów i typowych raportów dotyczących mienia komunalnego.

2) EGW - System Dzierżaw Wieczystych EGW jest przeznaczony do naliczania opłat za użytkowanie wieczyste gruntów, tworzenia i drukowania decyzji dotyczących opłat rocznych oraz do prowadzenia wieloletniego archiwum. W systemie przechowywane są zarejestrowane dane dotyczące podatników i ich kart podatkowych, udostępniane do przeglądania i modyfikacji.

3) ELUD+ - System jest przeznaczony do obsługi Lokalnego Banku Danych PESEL w zakresie zadań zleconych gminie. Służy do rejestracji i modyfikacji danych dotyczących ludności, przeprowadzania analiz i sprawozdawczości oraz emisji wyników, okresowej wymiany danych z systemami nadrzędnymi: Terenowym, Wojewódzkim oraz Centralnym Bankiem Danych, a także do udostępniania danych dotyczących ludności pozostałym systemom z pakietu RADIX: ewidencji gruntów, podmiotów gospodarczych, windykacji opłat i podatków itd.

4) EPOD - System Ewidencji Działalności Gospodarczej EPOD umożliwia prowadzenie ewidencji podmiotów gospodarczych i służy do drukowania zaświadczeń o wpisie do ewidencji, zmianach we wpisie do ewidencji, drukowania decyzji o wykreśleniu z ewidencji, o odmowie wpisu do ewidencji, sporządzania wykazów podmiotów gospodarczych i sporządzania zestawień statystycznych dotyczących ewidencji.

5) ESO - System Obsługi Stypendiów Oświatowych ESO+ przeznaczony jest do obsługi zadań związanych z przyznawaniem i realizacją stypendiów oświatowych - socjalnych oraz motywacyjnych, a także zasiłków jednorazowych.

6)FAKTURA - System służy do rejestracji i drukowania faktur i rachunków sprzedaży VAT, faktur i rachunków korygujących, prowadzenia kartoteki faktur, towarów i usług oraz kartoteki płatników, bieżącej aktualizacji kartotek, modyfikacji danych.

7) FKB+ - System Księgowości Budżetowej FKB służy do prowadzenia ksiąg rachunkowych wg klasyfikacji budżetowej, wspomagania prac nad budżetem jednostki samorządu terytorialnego, sporządzania wykazów obrotów i stanów kont w ujęciu analitycznym

i (sub)syntetycznym w dowolnym okresie czasu, sporządzania wymaganych przepisami sprawozdań z wykonania budżetu oraz do obsługi archiwum poprzednich lat.

8) INFO – system służy do udostępniania kierownictwu organu samorządowego syntetycznej informacji o osobach fizycznych i prawnych, zamieszkałych, posiadających własność lub prowadzących działalność gospodarczą na terenie gminy

9) KADRY - System KADRY służy do rejestracji danych osobowych pracowników, prowadzenia kartotek zawierających warunki i zasady zatrudnienia, przebieg pracy zawodowej, dane do ubezpieczenia ZUS i inne, prowadzenia ewidencji czasu pracy, drukowania dokumentów związanych z zatrudnieniem, automatycznego aktualizowania danych związanych z liczbą lat stażu pracy, należnym dodatkiem stażowym, nagrodą jubileuszową, wykonywania dowolnych analiz i wyciągów z bazy danych na podstawie określonych przez użytkownika warunków wyboru, a w powiązaniu z systemem PŁACE, również do automatycznego sporządzania list płac, wykazów podatkowych itp.

10) KASA - System KASA umożliwia kompleksową obsługę kasy. Służy do rejestracji wpłat gotówkowych i czekowych, wypłat należności, prowadzenia sprzedaży oraz obsługi wpłat i wypłat z wykorzystaniem drukarki fiskalnej, przygotowania dokumentów i rejestracji wpłat z możliwością wielokrotnych zmian organizacji pracy - na jednym lub kilku stanowiskach, drukowania raportów kasowych i bankowych dowodów wpłaty, wyodrębniania wpłat i wypłat dla zadań (jednostek) zarejestrowanych w systemie finansowo-księgowym FKB lub zdefiniowanych w systemie KASA, sporządzania wyciągów operacji kasowych przypisanych jednostkom z systemu FKB i prowadzenia wieloletniego archiwum.

11) PŁACE - System PŁACE służy do automatycznego sporządzania list płac zatrudnionych pracowników, obsługi składek ubezpieczeniowych wg zasad zgodnych z reformą ubezpieczeń społecznych, kartotek podatku dochodowego, drukowania zestawień płacowych, automatycznego naliczania zasiłków chorobowych, prowadzenia kart zasiłkowych i deklaracji rozliczeniowych ZUS. System emituje dane dla programu PŁATNIK ZUS i umożliwia prowadzenie wieloletniego archiwum.

12) POGRUN - System Naliczania Podatków od Gruntów i Nieruchomości POGRUN służy do naliczania podatku rolnego, leśnego i od nieruchomości, wprowadzania zmian i naliczania związanych z nimi przypisów i odpisów, wydruku postanowień o wszczęciu postępowania podatkowego, nakazów płatniczych, decyzji po zmianie i decyzji wymiarowych, prowadzenia wieloletniego archiwum wymiaru, rejestracji deklaracji podatkowych od osób prawnych oraz rejestracji zmian deklaracji.

13) POST - System Naliczania Podatków od Środków Transportu POST przeznaczony jest dla jednostek administracji samorządowej, które nie prowadzą ewidencji pojazdów, a obowiązane są naliczać podatek od środków transportu.

14) STW - System Środki Trwałe STW jest przeznaczony do obsługi zadań związanych z prowadzeniem ewidencji środków trwałych, wyposażenia oraz wartości niematerialnych i prawnych.

15) UPR - System Nadawania Uprawnień UPR służy do zabezpieczenia pakietu RADIX przed osobami nieuprawnionymi do jego obsługi. Umożliwia on zdefiniowanie wielu użytkowników o różnych prawach dostępu do poszczególnych programów pakietu.

16) WIP - System Windykacji Opłat i Podatków służy do zakładania i bieżącej aktualizacji kont rozrachunkowych dla wszystkich płatników z terenu gminy, księgowania operacji na poszczególnych kontach (przypisy, wpłaty, odpisy itp.) niezależnie od rodzaju podatku lub opłaty, tworzenia wykazów podatków i opłat, prowadzenia wieloletniego archiwum, analizy rozrachunkowej kont, obsługi tytułów wykonawczych oraz drukowania upomnień i decyzji.

17) WYB - System Rejestr Wyborców WYB służy do prowadzenia stałego rejestru wyborców wg zasad określonych przez Państwową Komisję Wyborców, emitowania spisu wyborców i okresowych meldunków dla PKW o stanie rejestru, drukowania zawiadomień związanych z prowadzeniem rejestru wyborców. Rejestr wyborców jest prowadzony w oparciu o dane zawarte w bazie ewidencji ludności systemu ELUD oraz o dane zarejestrowane na wniosek wyborcy.

18) System **ESOUSC** umożliwia całkowitą automatyzację podstawowych czynności wykonywanych w Urzędzie Stanu Cywilnego, począwszy od sporządzenia aktu, po wydawanie wszelkiego rodzaju dokumentów emitowanych na jego podstawie.

19) **System Straż Miejska STM** służy do prowadzenia kartotek funkcjonariuszy Straży Miejskiej, osób ukaranych, ujawnionych przestępstw, wydanych mandatów karnych, a także do tworzenia i drukowania zestawień mandatów kredytowych wraz z datą i potwierdzeniem ich wpłaty, zestawień dotyczących wyników wybranych funkcjonariuszy, oraz zestawień kar i wykroczeń popełnionych przez cudzoziemców wraz z informacją o kraju pochodzenia oraz rodzaju kary (wykroczenia).

Rozdział 2

Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności (§ 5 pkt 1 rozporządzenia)

§ 8

1. W urzędzie działa sieć oparta na systemie Windows Server 2003. 2.
2. Wszystkie komputery pracują w domenie (umig.b-ca.lokalna).
3. Każdy użytkownik uprawniony do pracy w systemie informatycznym posiada konto, zbudowane w następujący sposób: "imię.nazwisko" użytkownika (bez polskich liter). W momencie założenia nowego konta użytkownikowi, administrator nadaje hasło startowe złożone z minimum 9 znaków.
4. Zabrania się pracownikom ujawniania haseł jakimkolwiek osobom trzecim oraz zapisywania haseł lub takiego z nimi postępowania, które umożliwia lub ułatwia dostęp do haseł osobom trzecim.

Rozdział 3

Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem (§ 5 pkt 2 i 3 rozporządzenia).

§ 9

1. Po pierwszym zalogowaniu się użytkownika do domeny, system wymusza zmianę hasła. Obowiązek zmiany hasła wymusza kontroler domeny w cyklu 30 dniowym.
2. W przypadku zapomnienia przez użytkownika hasła dostępu do systemu, użytkownik zobowiązany jest poinformować o tym fakcie administratora sieci komputerowej, który uruchamia procedurę przydzielenia nowego hasła na zasadach określonych w ust. 1.

§ 10

1. Dodatkowe zabezpieczenie kontrolera domeny polega na limitowaniu czasu pracy stanowisk podłączonych do sieci. Kontroler domeny dopuszcza pracę na stanowiskach w godzinach pracy urzędu z marginesem jednej godziny.
2. W sytuacjach wyjątkowych administrator sieci, umożliwia pracę na stanowiskach w innych godzinach.

3. Jeżeli komputer na stanowisku jest zalogowany do systemu i nie wykazuje aktywności przez okres dłuższy niż 15 min. następuje jego blokada. Odblokowanie jest możliwe po podaniu aktualnego hasła użytkownika.
4. Użytkownik na stanowisku komputerowym, przed rozpoczęciem pracy z określonym programem musi podać swój login i hasło uprawniające go do korzystania z tego zasobu.
7. Administrator sieci komputerowej otrzymuje od kierownika określonego wydziału, wykaz nazwisk użytkowników wraz rodzajem uprawnień do korzystania z odpowiednich programów.
5. Użytkownicy w systemie są przypisani do określonej grupy, a ta z kolei ma nadane uprawnienia do otwierania aplikacji związanych z stanowiskiem służbowym.
6. Zakończenie pracy użytkownika w systemie następuje po „wylogowaniu się" z systemu. Po zakończeniu pracy użytkownik zabezpiecza swoje stanowisko pracy, w szczególności dyskietki, dokumenty i wydruki zawierające dane osobowe, przed dostępem osób nieupoważnionych.

Rozdział 4

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania (§ 5 pkt 4 i 5)rozporządzenia).

§ 11

1. Administrator sieci komputerowej codzienne tworzy pełne kopie bezpieczeństwa wszystkich zasobów systemu i przechowuje je przez kolejne 30 dni.
2. Kopie przechowywane są na dyskach twardych dwóch komputerów umieszczonych w prawidłowo zabezpieczonych pomieszczeniach w dwóch różnych punktach urzędu. Ponadto raz w miesiącu kopia umieszczana na nośniku CD, który przechowywany jest w szafie pancernej w Wydziale Organizacyjno - Prawnym.
3. Kopie bezpieczeństwa umieszczone na nośnikach CD przechowywane są przez okres 12 miesięcy, następnie są one fizycznie niszczone w obecności specjalnie powołanej komisji.
4. W przypadku konieczności wymiany dysku twardego, na którym tworzone są kopie, jest on również fizycznie niszczony w obecności komisji.

5. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przeznaczone do przekazania innemu podmiotowi, pozbawia się wcześniej zapisu tych danych.

Rozdział 5

Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, (§ 5 pkt 6 rozporządzenia).

§ 12

1. W urzędzie na każdym stanowisku komputerowym działa oprogramowanie antywirusowe, antyspamowe wraz z zaporą internetową.
2. Punktem styku sieci wewnętrznej z zewnętrzną jest router, na którym zainstalowany jest system operacyjny Linux. Zainstalowana na nim zapora chroni przed niepożądanymi użytkownikami z zewnątrz sieci.

§ 13

Oprogramowanie na komputerach może być zainstalowane wyłącznie przez informatyków. W przypadku zainstalowania oprogramowania bez odpowiedniej akceptacji pracownik ponosi odpowiedzialność porządkową i prawną.

Rozdział 6

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych (§ 5 pkt 8 rozporządzenia)

§ 14

1. W przypadku przekazywania do naprawy nośników informatycznych zawierających dane osobowe dyski lub inne elektroniczne nośniki informacji, przeznaczone do naprawy, pozbawiane są wcześniej zapisanych danych w sposób uniemożliwiający ich odzyskanie.
2. Czynności związane z konserwacją systemu informatycznego wykonywane są raz w miesiącu przez informatyków urzędu.
3. Likwidacja bądź przekazanie sprzętu komputerowego, na którym przetwarza się dane osobowe następuje po całkowitym pozbawieniu zapisu danych bądź uszkodzenie w sposób uniemożliwiający ich odczytanie.

Rozdział 7

Postępowanie w przypadku stwierdzenia naruszenia zabezpieczania systemu informatycznego

§ 15

Użytkownik systemu informatycznego zobowiązany jest zawiadomić administratora bezpieczeństwa systemu informacji, o każdym naruszeniu zabezpieczenia systemu polegającym na:

1) naruszeniu hasła dostępu (system nie reaguje na hasło lub je ignoruje – usunięty mechanizm hasła),
2) częściowym lub całkowitym braku bazy danych,
3) braku możliwości uruchomienia właściwej aplikacji (programu komputerowego),
4) zmianie położenia sprzętu komputerowego lub możliwości połączenia wszystkich urządzeń,
5) przebywanie osób nieuprawnionych wewnątrz obszaru przetwarzania danych osobowych,
6) inne zdarzenia mogące mieć wpływ na naruszenie systemu informatycznego.

§ 16

1. Administrator bezpieczeństwa informacji, po otrzymaniu zawiadomienia o naruszeniu zabezpieczenia systemu informatycznego powinien niezwłocznie:
   1) przeprowadzić postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia ochrony danych osobowych,
   2) podjąć działania w celu usunięcia uchybień oraz zastosować dodatkowe środki zabezpieczające system przed ponownym naruszeniem zabezpieczenia,
   3) sporządzić protokół dokonanych czynności.
2. Protokół, o którym mowa w ust.1 pkt 3, przekazuję się niezwłocznie, jednakże nie później niż w ciągu 3 dni administratorowi danych osobowych

§ 17

1. W przypadku kradzieży sprzętu informatycznego z pomieszczeń, w których przetwarzane są dane osobowe użytkownik, niezwłocznie powiadamia kierownika merytorycznego wydziału oraz administratora bezpieczeństwa informacji.
2. W sytuacji, o której mowa w ust.1, administrator bezpieczeństwa informacji podejmuje czynności określone w § 16.

§ 18

W sytuacji , o której mowa w § 16 i 17, decyzję o dalszym trybie postępowaniu w zakresie powiadomienia właściwych organów oraz podjęcia innych, szczególnych czynności zabezpieczających wskazania podejmuje administrator danych osobowych, po zapoznaniu się z protokołem, o którym mowa w § 16 ust. 1 pkt 3.

§ 19

1. Informatyk jest zobowiązany na bieżąco informować administratora bezpieczeństwa informacji o przypadkach awarii programowych wynikających z:
   1) posługiwania się przez użytkowników nieautoryzowanymi programami,
   2) nie przestrzegania zasad używania programów antywirusowych w określonych okolicznościach ,
   3) niewłaściwego wykorzystywania sprzętu komputerowego.
2. Administrator bezpieczeństwa informacji składa okresowo, nie rzadziej niż raz na rok, administratorowi danych osobowych, kompleksową analizę zarządzania systemem informatycznym służącym przetwarzaniu danych osobowych oraz założenia strategii i polityki zabezpieczenia systemów informatycznych.

§ 20

1. Dokumenty systemu informatycznego , w szczególności zawierające opis parametrów technicznych oraz rozwiązania systemowe, zapewniające ochronę poufności, integralności i rozdzielczości są informacją niejawną oznaczoną klauzulą „poufne".
2. Dokumenty, o których mowa w ust.1 są przygotowywane i wdrażane przez administratora bezpieczeństwa systemu.