ZARZĄDZENIE NR 119/2007

Burmistrza Miasta i Gminy Opatów

z dnia 05 listopada 2007r.

w sprawie wprowadzenia w Urzędzie Miasta i Gminy w Opatowie

Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych,
Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz Polityki bezpieczeństwa przetwarzania danych osobowych.

Na podstawie art. 36 ust. 2 Ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. z 2002r. Nr 101, poz. 926 z późniejszymi zmianami), Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w 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 2004r. Nr 100, poz. 1024)

zarządzam, co następuje:

§ 1

W celu określenia zasad, sposobu i procedur ochrony danych osobowych w Urzędzie Miasta i Gminy w Opatowie wprowadzam do użytku i stosowania:

1). Instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych stanowiącą załącznik Nr 1.
2). Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych stanowiącą załącznik Nr 2.
3). Politykę bezpieczeństwa przetwarzania danych osobowych stanowiącą załącznik Nr 3.

§ 2

Nadzór nad przestrzeganiem oraz właściwym stosowaniem w/w instrukcji sprawują wszyscy kierownicy referatów Urzędu Miasta i Gminy w Opatowie, w których przetwarza się dane osobowe.

§ 3

Zarządzenie wchodzi w życie z dniem 12 listopada 2007r.

BURMISTRZ
mgr Krystyna Kielisz

Załącznik Nr 1
do Zarządzenia Nr 119/2007
Burmistrza Miasta i Gminy Opatów
z dnia 05 listopada 2007r

Instrukcja
postępowania w sytuacji naruszenia ochrony danych osobowych

Rozdział I
Postanowienia ogólne

§ 1

1). Niniejsza Instrukcja, (zwana dalej: instrukcją), jest wewnętrznym dokumentem Urzędu Miasta i Gminy w Opatowie, (zwanym dalej: Urzędem) i jest przeznaczona dla osób zatrudnionych przez Urząd przy przetwarzaniu danych osobowych.
2). Przestrzeganie postanowień instrukcji służyć ma wykrywaniu i właściwemu reagowaniu na przypadki naruszenia ochrony danych osobowych w Urzędzie.

§ 2

Następujące słowa, użyte w Instrukcji, oznaczają:
1). **administrator danych** – Burmistrz Miasta i Gminy Opatów;
2). **administrator bezpieczeństwa informacji** (zwany też dalej: **ABI)** - osoba wyznaczona przez Burmistrza, odpowiedzialna za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń;
3). **osoba upoważniona lub użytkownik** – osoba posiadająca upoważnienie wydane przez administratora i dopuszczona w zakresie w nim wskazanym, jako użytkownik do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych lub uprawniona we wskazanym zakresie do dostępu do danych osobowych;
4). **osoba trzecia** – to każda osoba nieupoważniona i przez to nieuprawniona do dostępu do danych osobowych lub zbiorów tych danych, w tym w szczególności interesanci Urzędu;
5). **dane osobowe** - wszelka dokumentacja zawierająca dane osobowe;
6). **system informatyczny**- system przetwarzania danych osobowych w Urzędzie;
7). **zabezpieczenie systemu informatycznego** – wdrożenie w Urzędzie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą.

§ 3

1. Naruszenie ochrony danych osobowych w Urzędzie ma miejsce w każdym przypadku, gdy:
   1). Stwierdzono naruszenie zabezpieczenia systemu informatycznego;
   2). Stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu mogą wskazywać na naruszenie zabezpieczeń tych danych;
   3). Gdy stan pomieszczeń i szaf bądź innych mebli biurowych, w których przechowuje się akta lub nośniki informacji oraz zawartości tych akt lub nośników informacji wzbudzają podejrzenie, że dostęp do nich mogły mieć osoby trzecie. (zwanych dalej: **naruszeniami ochrony**)

2. O przypadkach naruszeń ochrony, o których mowa w ust. 1 pkt. 1) i 2), osoba zatrudniona w Urzędzie obowiązana jest niezwłocznie powiadomić ABI lub inną upoważnioną przez niego osobę.
3. O przypadkach naruszeń ochrony, o których mowa w ust. 1 pkt. 3), osoba zatrudniona w Urzędzie obowiązana jest niezwłocznie powiadomić swojego przełożonego lub ABI lub inną upoważnioną przez niego osobę.

§ 4

Naruszenie ochrony, o którym mowa w § 3 ust.1 pkt. 3), może przejawiać się w szczególności w postaci:

1). widocznych uszkodzeń, bądź naruszeń powierzchni drzwi, szaf lub innych mebli biurowych lub ich zamknięć;
2). uszkodzeniu nośnika informacji, budzące podejrzenie iż do ich treści mogły mieć dostęp osoby trzecie;
3). nieuprawnionego dostępu lub próby dostępu do systemu lub pomieszczeń,
4). naruszeniu lub próbie naruszenia integralności systemu,
5). zmiany lub utraty danych zapisanych na kopiach zapasowych lub archiwalnych dokonanej w sposób nieautoryzowany,
6). zniszczenie oraz próby zniszczenia w sposób nieautoryzowany danych zgromadzonych w systemie,
7). innego stanu systemu lub pomieszczeń niż pozostawiony przez użytkownika po zakończeniu lub po przerwie w pracy z systemem.

Rozdział II
Przedsięwzięcia zabezpieczające przed naruszeniem systemu ochrony danych osobowych

§ 5

W celu uniemożliwienia osobom nieuprawnionym dostępu do zbioru danych osobowych, których administratorem jest Urząd Miasta i Gminy w Opatowie dokonano identyfikacji możliwych zagrożeń, podjęto stosowne przedsięwzięcia, których celem jest zapewnienie odpowiednich standardów zabezpieczeń systemu ochrony danych osobowych przed jego naruszeniem.

§ 6

Do przedsięwzięć, o których mowa w § 5, należą przede wszystkim:

1). zabezpieczenie wejścia do lokalu stanowiącego siedzibę Administratora danych zamkami.
2). wyposażenie pomieszczeń w szafy zabezpieczone przed otwarciem kłódkami lub zamkami,

§ 7

1). Stały dostęp do pomieszczeń mają tylko użytkownicy.
2). Klucze do szaf, w których przechowywane są dane osobowe powinny być umieszczane w specjalnie w tym celu wydzielonej szafie, którą zamyka się po zakończeniu pracy.

Rozdział III

Postępowanie w przypadku naruszenia zabezpieczenia systemu ochrony danych osobowych

§ 8

1. Do czasu przybycia Administratora Bezpieczeństwa Informacji lub upoważnionej przez niego osoby, zgłaszający:
   1) zabezpiecza dostęp do miejsca lub urządzenia przez osoby trzecie;
   2) wstrzymuje pracę na komputerze, na którym zaistniało naruszenie ochrony oraz nie uruchamiania bez koniecznej potrzeby komputerów i innych urządzeń, które w związku z naruszeniem ochrony zostały wstrzymane;
   3) nie zmienia położenia przedmiotów, które pozwalają stwierdzić naruszenie ochrony lub odtworzyć jego okoliczności.
   4) podejmuje, stosownie do zaistniałej sytuacji, inne niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.
2. Postanowienia ust. 1 mają odpowiednie zastosowanie w przypadku naruszenia lub podejrzenia naruszenia integralności danych osobowych.

§ 9

Zgodę na uruchomienie komputerów i innych urządzeń lub dokonanie zmian w miejscu naruszenia ochrony wyraża administrator bezpieczeństwa informacji lub inna upoważniona przez niego osoba.

§ 10

Okoliczności i przyczyny naruszeń ochrony ustala zespół, w którego skład wchodzi Administrator bezpieczeństwa informacji i Administrator danych osobowych, w którym nastąpiło naruszenie ochrony.

§ 11

Niezwłocznie po otrzymaniu wiadomości o naruszeniu ochrony zespół, o którym mowa w § 10, przystępuje do ustalenia okoliczności i przyczyn tego naruszenia, a w szczególności:

1). dokonuje oględzin miejsca naruszenia, bądź urządzenia, w którym wykryto naruszenie oraz bada inne okoliczności, które mogły mieć wpływ na powstanie naruszenia ochrony;
2). wysłuchuje relacji osoby zatrudnionej przy przetwarzaniu danych, która dokonała powiadomienia,
3). jeżeli jest to konieczne, sporządza szkic lub wykonuje fotografię miejsca naruszenia ochrony,
4). podejmuje decyzje o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych.

§ 12

1). Zespół, o którym mowa w § 10, z czynności, o których mowa w § 11 sporządza protokół oględzin, który stanowi podstawę do:
- ustalenia skali stwierdzonych naruszeń ochrony, przyczyn ich powstania, skutków, jakie wywołują lub mogą wywołać, w odniesieniu do stanu zabezpieczenia danych osobowych;

- wyciągnięcia wniosków, zwłaszcza co do podjęcia określonych działań organizacyjnych i technicznych.

2). Protokół oględzin, o którym mowa w ust. 1, zespół, o którym mowa w § 10, podejmuje decyzję o koniecznych działaniach organizacyjnych i technicznych.

§ 13

Po zaistnieniu okoliczności, o których mowa w § 4, wskazujących na naruszenie bezpieczeństwa danych, osoba zatrudniona przy przetwarzaniu danych może kontynuować pracę dopiero po otrzymaniu pozwolenia od Administratora bezpieczeństwa informacji.

§ 14

Administrator bezpieczeństwa informacji lub upoważniona przez niego osoba podejmuje kroki zmierzające do likwidacji naruszeń ochrony systemu i zapobieżenia wystąpieniu ich w przyszłości.

W tym celu :

1). W miarę możliwości przywraca stan zgodny z zasadami zabezpieczenia systemu,

2). Relacjonuje Burmistrzowi przedsięwzięte czynności,

3). O ile taka potrzeba zachodzi, postuluje wprowadzenie nowych form zabezpieczenia systemu, a w razie ich wprowadzenia zaznajamia z nimi osoby zatrudnione przy przetwarzaniu danych.

Rozdział IV

Postanowienia końcowe

§ 15

Instrukcja wchodzi w życie z dniem jej wprowadzenia w Urzędzie Miasta i Gminy w Opatowie, określonym w Zarządzeniu Burmistrza Miasta i Gminy Opatów.

BURMISTRZ
mgr Krystyna Kielisz

Załącznik Nr 2
do Zarządzenia 119/2007
Burmistrza Miasta i Gminy Opatów
z dnia 05 listopada 2007r.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Rozdział I
Postanowienia ogólne

§ 1

Niniejsza Instrukcja, (zwana dalej: **instrukcją**), jest wewnętrznym dokumentem Urzędu Miasta i Gminy w Opatowie i ma zastosowanie do wszelkich danych osobowych znajdujących się, bądź mogących znajdować się w systemie informatycznym Urzędu.

§ 2

Instrukcja określa, w szczególności:

1). Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;

2). Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;

3). Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;

4). Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;

5). Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych, o których mowa w pkt 4).,

6). Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do ROZPORZĄDZENIA MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI (Dz. U. z 2004 r. Nr100 poz.1024)

7). Sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 ROZPORZĄDZENIA MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI (Dz. U. z 2004 r. Nr100 poz.1024)

8). Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

§ 3

Instrukcja ma na celu zapewnienie procedur i właściwych warunków zarządzania systemem informatycznym dla ochrony zgromadzonych tam danych, jak również jednolitych i bezpiecznych zasad korzystania z danych osobowych przetwarzanych w systemie informatycznym oraz w aktach Urzędu.

§ 4

Realizację zamierzeń określonych w § 3 gwarantuje następująca strategia:

1). Przeszkolenie użytkowników w zakresie ochrony danych osobowych oraz zaznajomienie z przepisami dotyczącymi ochrony danych osobowych,

2). Korzystanie z oprogramowania systemowego i użytkowego najnowszej generacji,

3). Zainstalowanie w systemie informatycznym zabezpieczeń gwarantujących nienaruszoną pracę systemu,

4). Przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasła i identyfikatory),

5). Ocena ewentualnych zagrożeń bezpieczeństwa systemu informatycznego i ryzyk związanych z jego obsługą,

6). Wdrożenie zabezpieczeń o charakterze fizycznym pomieszczeń, stosownie do zagrożeń i ryzyk wynikających z oceny, o której mowa w pkt 5,

7). Stałe monitorowanie wdrożonych zabezpieczeń w celu identyfikacji podatnych na zagrożenia obszarów i słabości zabezpieczeń,

§ 5

Następujące słowa, użyte w Instrukcji, oznaczają:

1). **administrator danych** – Burmistrz Miasta i Gminy Opatów
   - Kierownik Referatu Spraw Obywatelskich
   - Kierownik Referatu Organizacyjnego
   - Kierownik Referatu Finansowego
   - Kierownik Referatu Rozwoju Gminy, Rolnictwa i Nadzoru Komunalnego
   - Kierownik Urzędu Stanu Cywilnego

2). **administrator bezpieczeństwa informacji** - osoba wyznaczona przez Burmistrza , odpowiedzialna za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń;

3). **osoba upoważniona lub użytkownik** – osoba posiadająca upoważnienie wydane przez Administratora Danych i dopuszczona w zakresie w nim wskazanym, jako użytkownik do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych;

4). **osoba trzecia** – to każda osoba nieupoważniona i przez to nieuprawniona do dostępu do danych osobowych lub zbiorów tych danych,

5). **system informatyczny** - system przetwarzania informacji w Urzędzie wraz ze związanymi z nim ludźmi oraz zasobami technicznymi, który dostarcza i rozprowadza informacje,

6). **zabezpieczenie systemu informatycznego** – wdrożenie w Urzędzie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą.

Rozdział II

Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

§ 6

1). Rejestracji i wyrejestrowywania użytkowników dokonuje Administrator bezpieczeństwa informacji, który prowadzi ewidencję.

2). Identyfikator użytkownika w aplikacji jest tożsamy z tym, jaki jest mu przydzielany w sieci lokalnej.

3). Ewidencja zawiera:
- Imię i nazwisko użytkownika
- Data otrzymania identyfikatora
- Data wyrejestrowania użytkownika
- Identyfikator

4). Jakakolwiek zmiana w zakresie informacji zawartych w ewidencji podlega natychmiastowemu odnotowaniu.

§ 7

Dana osoba jest rejestrowana w systemie informatycznym, jako użytkownik po spełnieniu następujących warunków:
Uzyskaniu przez tą osobę - upoważnienia wydanego przez Administratora dopuszczającego daną osobę w zakresie w nim wskazanym, jako użytkownika, do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych,

§ 8

1). Z chwilą zarejestrowania w systemie informatycznym, zgodnie z postanowieniami § 7, dana osoba jest informowana przez Administratora bezpieczeństwa informacji o ustalonym dla niej identyfikatorze i konieczności posługiwania się hasłami

2). Bez spełnienia wymogów wynikających z postanowień § 7 Administrator bezpieczeństwa informacji nie może zarejestrować jakiejkolwiek osoby w systemie informatycznym.

§ 9

1. Użytkownik jest wyrejestrowywany z systemu informatycznego w każdym przypadku utraty przez niego uprawnień do dostępu do danych osobowych, co ma miejsce w przypadku:
   - ustania zatrudnienia tego użytkownika w Urzędzie – o czym informację Administrator bezpieczeństwa informacji uzyskuje od upoważnionego pracownika Urzędu,
   - zmiany zakresu obowiązków tego użytkownika - o czym informację Administrator bezpieczeństwa informacji uzyskuje od przełożonego użytkownika.
2. Poza przypadkami wskazanymi w ust. 1 użytkownik jest wyrejestrowywany z systemu informatycznego w każdym przypadku odwołania przez Administratora wydanego temu użytkownikowi upoważnienia.

§ 10

W przypadkach wskazanych w § 9 Administrator bezpieczeństwa informacji, co do użytkownika, który utracił uprawnienia do dostępu do systemu informatycznego, dokonuje niezwłocznie następujących czynności:

1). Blokuje jego profil, co powoduje, że osoba ta nie ma możliwości „zalogowania się" do sieci lub aplikacji;

2). Wyrejestrowuje jego identyfikator;
3). Unieważnia jego hasło;

§ 11

1). Identyfikator, który utracił ważność nie może być ponownie przydzielony innemu użytkownikowi,

§ 12

Administrator bezpieczeństwa informacji ustala swoje hasło wg zasad ustalania hasła dla użytkownika.

§ 13

Hasło administratora bezpieczeństwa informacji jest przechowywane w zaklejonej i opieczętowanej kopercie w kasie pancernej znajdującej się w pok. Nr 11a.

§ 14

W przypadku nieobecności administratora bezpieczeństwa informacji w sytuacji awaryjnej administrator danych wyznacza osobę, która usunie awarię. Login oraz hasło administratora bezpieczeństwa informacji wprowadza administrator danych w sposób uniemożliwiający poznanie go przez osoby postronne.

Rozdział III

Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;

§ 15

Mając na względzie, iż system informatyczny przetwarzający dane osobowe powinien być wyposażony w mechanizmy uwierzytelnienia użytkownika oraz kontroli dostępu do tych danych dla każdej osoby upoważnionej ustalany jest odrębny identyfikator i hasło, tak aby bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym mógł mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
W systemie informatycznym stosuje się uwierzytelnianie dwustopniowe; na poziomie:

1). dostępu do sieci lokalnej,

2). dostępu do aplikacji.

Hasła dostępu i identyfikatory przyznawane są indywidualnie dla każdego z użytkowników i znane tylko właścicielowi.

§ 16

Identyfikator użytkownika:

1). Jest niepowtarzalny
2). Po wyrejestrowaniu użytkownika z systemu informatycznego Urzędu nie jest przydzielany innej osobie;
3). Nie podlega zmianie,
4). Jest wpisywany do ewidencji osób zatrudnionych przy przetwarzaniu danych wraz z imieniem i nazwiskiem użytkownika oraz jest rejestrowany w systemie informatycznym Urzędu.
5). Za przydział identyfikatora odpowiada Administrator bezpieczeństwa informacji

§ 17

Hasło użytkownika:

1). Jest przydzielane indywidualnie dla każdego z użytkowników i znane tylko użytkownikowi, który się nim posługuje,
2). Nie jest zapisywane w systemie w postaci jawnej,
3). Jest zmieniane, co najmniej raz na miesiąc,
4). Jest utrzymywane w tajemnicy, również po upływie jego ważności.

§ 18

Osobą odpowiedzialną w Urzędzie za sposób przydziału haseł dla użytkowników i częstotliwość ich zmiany jest Administrator bezpieczeństwa informacji,

§ 19

Przydziału i zmiany haseł dokonuje się w następujący sposób:
1). Wymogiem niezbędnym jest przydział haseł skonstruowanych co najmniej z 6 (sześciu) znaków,
2). Zmianę haseł dostępu do sieci lokalnej wymusza co najmniej raz na 30 dni, serwer.
3). Hasła dostępu do aplikacji są zmieniane przez każdego z użytkowników co najmniej raz na 30 dni.
4). Zachowując wymóg zmieniania haseł każdego z użytkowników co najmniej raz na 30 dni, hasła użytkowników nie mogą się powtarzać.
5). Hasła nie mogą składać się z kombinacji znaków mogących prowadzić do odszyfrowania ich przez osoby nieupoważnione
6). Niezależnie od wymogu zmieniania haseł każdego z użytkowników co najmniej raz na 30 dni, hasło winno być zmienione przez użytkownika niezwłoczne w przypadku powzięcia podejrzenia lub stwierdzenia, że z hasłem mogły zapoznać się osoby trzecie.

§ 20

1). Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu hasła, którym się posługuje lub posługiwał.
2). Użytkownik obowiązany jest utrzymywać hasła, którymi się posługuje lub posługiwał w ścisłej tajemnicy, co obejmuje, w szczególności dołożenie przez niego wszelkich starań w celu uniemożliwienia zapoznania się przez osoby trzecie z hasłem nawet po ustaniu jego ważności, czy też użycia hasła przez te osoby.
3). W przypadku powzięcia przez użytkownika podejrzenia lub stwierdzenia ze z hasłem mogły zapoznać się osoby trzecie, obowiązany jest on niezwłocznie zmienić hasło i powiadomić o tym Administratora bezpieczeństwa informacji.
4). Naruszenie przez użytkownika postanowień ust. 2 lub 3 może stanowić podstawę dla pociągnięcia użytkownika do odpowiedzialności dyscyplinarnej, odszkodowawczej lub karnej w trybie i na zasadach przewidzianych przepisami prawa.
5). Użytkownicy obowiązani są utrzymywać hasła w tajemnicy również po upływie ich ważności

Rozdział IV
Procedury rozpoczęcia, zawieszenia i zakończenia pracy,

§ 21

1). Przed przystąpieniem do pracy w systemie użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych służących do przetwarzania danych osobowych oraz dokonać oględzin swojego stanowiska pracy, ze szczególnym uwzględnieniem czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.
2). W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie systemu, każdy pracownik ma obowiązek powiadomić Administratora Bezpieczeństwa.

§ 22

1). Każdy użytkownik obowiązany jest "zalogować się" do sieci lokalnej, podając swój identyfikator i hasło dostępu.
2). Aby uruchomić aplikację wykorzystywaną do pracy w Urzędzie, należy podać swój identyfikator i hasło dostępu.
3). Bez wykonania procedury opisanej w ust.1 i 2 jakakolwiek praca w systemie komputerowym Urzędu nie jest możliwa.

§ 23

1). Maksymalna ilość prób wprowadzenia identyfikatora i hasła przy logowaniu się do lokalnej sieci i aplikacji wynosi 3.
2). Po błędnej próbie logowania do lokalnej sieci lub aplikacji, użytkownik otrzymuje komunikat o błędnym identyfikatorze lub haśle.
3). Użytkownik informuje Administratora bezpieczeństwa informacji o fakcie niemożliwości wejścia do systemu.
4). Administrator bezpieczeństwa informacji ustala przyczyny zablokowania systemu oraz, w zależności od zaistniałej sytuacji, podejmuje odpowiednie działania.

§ 24

1). W przypadku bezczynności użytkownika na komputerze stacjonarnym przez okres dłuższy niż 5 minut automatycznie włączany jest wygaszacz ekranu.
2). Przed opuszczeniem miejsca pracy, użytkownik obowiązany jest poczekać, aż zaktywizuje się wygaszacz.
3). W przypadku, gdy przerwa w pracy trwa dłużej niż 30 minut, oraz kończąc pracę użytkownik obowiązany jest „wylogować się" z aplikacji i systemu komputerowego Urzędu oraz sprawdzić czy nie zostały pozostawione bez zamknięcia nośniki informacji. Opuszczając stanowisko użytkownik zamyka używane przez niego szafy i pomieszczenia, w których przechowuje się akta i nośniki informacji.

§ 25

W przypadku zauważenia przez użytkownika naruszenia zabezpieczenia systemu informatycznego lub zauważenia, że stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu mogą wskazywać na naruszenie zabezpieczeń danych osobowych, użytkownik ten obowiązany jest poinformować o tym fakcie Administratora Bezpieczeństwa.

Rozdział V
Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

§ 26

Nośniki informacji zawierające dane osobowe są archiwizowane przez Administratora bezpieczeństwa informacji.

§ 27

Administrator bezpieczeństwa informacji obowiązany jest przestrzegać terminów sporządzania kopii zapasowych oraz okresowo dokonywać kontroli możliwości odczytu danych zapisanych na tych kopiach.

§ 28

Kopie awaryjne są:
1). Tworzone raz w tygodniu na odpowiednio opisanych i oznakowanych nośnikach magnetycznych
2). Raz w miesiącu sprawdzane pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu informatycznego Urzędu.

Rozdział VI
Sposób, miejsce i czas przechowywania kopii zapasowych oraz wydruków.

§ 29

Nie należy magazynować zbędnych plików i wydruków.

§ 30

Wydruki, zawierające dane osobowe, należy przechowywać w pokojach stanowiących obszar przetwarzania danych osobowych,

§ 31

Za zniszczenie zbędnych wydruków i innych dokumentów zawierających dane osobowe odpowiedzialny jest administrator danych, za skasowanie danych lub zniszczenie nośników informatycznych odpowiedzialny jest Administrator bezpieczeństwa informacji.

§ 32

Kopie bezpieczeństwa na nośnikach magnetycznych są przechowywane w zamkniętej szafie pancernej (pok. 11a).

§ 33

Zbędne dokumenty manualne (papierowe) powinny być zniszczone w niszczarce dokumentów lub podarte na drobne fragmenty.

§34

1). Urządzenia, dyski lub inne informatyczne nośniki informacji, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie, czego dokonać można w szczególności poprzez zniszczenie ich w sposób trwały, tj. przez ich mechaniczne zniszczenie.
2). Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych, pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający odczyt.

§35

1). Kopie zapasowe po ustaniu ich użyteczności; są bezzwłocznie usuwane
2). Kopie tygodniowe kasowane są po miesiącu.
3). Kopie zapasowe, które uległy uszkodzeniu podlegają natychmiastowemu zniszczeniu
4). Niszczenia kopii zapasowych, na nośnikach magnetycznych, dokonuje Administrator bezpieczeństwa informacji lub upoważniona przez niego osoba.
5). Z nośników magnetycznych dane należy usunąć w sposób uniemożliwiający ich odczytanie, a w przypadku, gdy usunięcie danych nie jest możliwe, nośniki podlegają zniszczeniu w stopniu uniemożliwiającym dostęp do zawartych na nich danych.
6). Z nośników podlegających zniszczeniu nie wolno sporządzać wydruków.

Rozdział VII

Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI (Dz.U. z 2004 r. Nr 100 poz. 1024)

§ 36

1). Sprzęt komputerowy obsługujący zbiór danych osobowych podłączony jest d o sieci elektrycznej za pomocą UPS-ów.
2). System informatyczny nie jest podłączony do sieci publicznej, chroniony programowym firewall-em oraz programem antywirusowym.

Rozdział VIII

Realizacja wymogów § 7 ust 1 pkt 4 ROZPORZĄDZENIA MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI (Dz.U. z 2004 r. Nr 100 poz. 1024).

§ 37

1). Systemy informatyczne posiadające funkcję, która pozwala na odnotowanie informacji określonej w § 7 ust 1 pkt 4 ROZPORZĄDZENIA MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI (Dz.U. z 2004 r. Nr 100 poz. 1024):
   - Windykacja należności podatkowych –WIP
   - Zbiór -rejestr ksiąg urodzeń, małżeństw i zgonów w USC – PB_USC
   - Łączne zobowiązanie pieniężne - POGRUN
   - Ewidencja ludności ELUD +

2). Systemy informatyczne nie posiadające funkcji, która pozwala na odnotowanie informacji określonej w § 7 ust 1 pkt 4 (dane z tych zbiorów nie są udostępniane) ROZPORZĄDZENIA MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI (Dz.U. z 2004 r. Nr 100 poz. 1024) :

- Rejestr Wyborców WYB+
- Ewidencja gruntów i budynków miasta i gminy Opatów – EWOPIS
- Ewidencja dowodów osobistych – System Wydawania Dowodów Osobistych
- Podatek od środków transportowych - POST

Rozdział IX

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

§ 38

1). Przeglądy i konserwacje sprzętu komputerowego dokonuje się w miarę potrzeb wynikających z obciążenia sprzętu komputerowego, warunków w których eksploatowane są dane urządzenia oraz ważności sprzętu.
2). Bieżące przeglądy, konserwacje oraz naprawy dokonywane są przez Administratora systemu informatycznego.

§ 39

Urządzenia, dyski lub inne informatyczne nośniki informacji, przeznaczone do napraw, gdzie wymagane jest zaangażowanie autoryzowanych firm zewnętrznych, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej przez Administratora bezpieczeństwa informacji.

Rozdział X
Postanowienia końcowe

§ 40

Instrukcja wchodzi w życie z dniem jej wprowadzenia w Urzędzie Miasta i Gminy w Opatowie, określonym w Zarządzeniu Burmistrza Miasta i Gminy Opatów.

BURMISTRZ
mgr Krystyna Kielisz

Załącznik Nr 3
do Zarządzenia Nr 119/2007
Burmistrza Miasta i Gminy Opatów
z dnia 05 listopada 2007r.

Polityka bezpieczeństwa przetwarzania danych osobowych.

Rozdział I

Postanowienia ogólne

§ 1

Niniejszy dokument, (zwany dalej: polityką bezpieczeństwa), jest wewnętrznym dokumentem Urzędu Miasta i Gminy w Opatowie i ma zastosowanie do wszelkich danych osobowych znajdujących się, bądź mogących znajdować się w systemie informatycznym urzędu.

§ 2

Polityka bezpieczeństwa zawiera w szczególności:

Wykaz pomieszczeń tworzący obszar, w którym przetwarzane są dane osobowe (Rozdział III);
Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych (Rozdział IV);
Opis struktury zbiorów danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi (Rozdział V);
Sposób przepływu danych pomiędzy poszczególnymi systemami eksploatowanymi w urzędzie (Rozdział VI);
Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych (Rozdział VII).

Rozdział II

Wstęp

§ 3

System informatyczny składa się z kilku aplikacji, które służą do wspomagania pracy w urzędzie.
W systemie są przetwarzane informacje stanowiące dane osobowe w rozumieniu art. 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Z 2002 r. Nr 101, poz. 926 z późn. zm.)
Osobą odpowiedzialną za właściwy i niezakłócony przebieg przetwarzania danych w tym systemie jest Burmistrz Miasta i Gminy w Opatowie.

Definicje

§ 4

Ilekroć mowa w niniejszym dokumencie o:

1). Urzędzie – należy przez to rozumieć Urząd Miasta i Gminy w Opatowie

2). Administratorze Bezpieczeństwa Informacji (ABI) – osoba wyznaczona przez Burmistrza, odpowiedzialna za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.
3). użytkowniku systemu – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie.
4). Administratorze Systemu Informatycznego (ASI) – należy przez to rozumieć pracownika odpowiedzialnego za funkcjonowanie systemu informatycznego oraz stosowanie technicznych i organizacyjnych środków ochrony stosowanych w tym systemie,
5). sieci lokalnej – należy przez to rozumieć połączenie systemów informatycznych urzędu

Rozdział III

Obszar przetwarzania danych osobowych

§ 5

Obszar przetwarzania danych osobowych w systemie informatycznym Urzędu Miasta i Gminy w Opatowie stanowią pokoje: 8, 10, 11A, 13, 14, 14a, 20, 22 oraz 22a mieszczące się w Urzędzie Miasta i Gminy w Opatowie, Kopie baz danych przechowywane są w kasie pancernej pokój nr 11A. Zbiory Tradycyjne będące zbiorem danych osobowych przechowywane są w pokoju 8, 9, 14, 14a, 20 i 20a w zamykanych na klucz szafach.

Rozdział IV

Wykaz zbiorów danych osobowych przetwarzanych w urzędzie.

§ 6

Dane zebrane są w następujących zbiorach:

1). **Rejestr użytkowników i współużytkowników wieczystych gruntów gminy Opatów – zbiór tradycyjny**
2). **Rejestr wydanych decyzji dotyczących rozgraniczenia nieruchomości – zbiór tradycyjny**
3). **Rejestr sprzedanych lokali mieszkalnych – zbiór tradycyjny**
4). **Rejestr zawartych umów dzierżawy – zbiór tradycyjny**
5). **Wykaz przedpoborowych – zbiór tradycyjny**
6). **Wykaz poborowych – zbiór tradycyjny**
7). **Windykacja należności podatkowych –WIP – Radix Gdańsk**
8). **Zbiór -rejestr ksiąg urodzeń, małżeństw i zgonów w USC – PB_USC Technika Gliwice**
9). **Rejestr zezwoleń na sprzedaż i podawanie napojów alkoholowych – zbiór tradycyjny**
10). **Podatek od środków transportowych - POST – Radix Gdańsk**
11). **Łączne zobowiązanie pieniężne - POGRUN – Radix Gdańsk**
12). **Ewidencja ludności ELUD + – Radix Gdańsk**
13). **Rejestr Wyborców WYB+ – Radix Gdańsk**
14). **Ewidencja dowodów osobistych - SystemWydawania Dowodów Osobistych – WASCO S.A.**
15). **Rejestr wydanych decyzji o warunkach zabudowy i zagospodarowaniu terenu**
16). **Rejestr użytkowników wieczystych, którym przekształcono użytkowanie wieczyste w prawo własności – zbiór tradycyjny**
17). **Ewidencja gruntów i budynków miasta i gminy Opatów – EWOPIS – GEOBID Gliwice**

18). **Rejestr przedsiębiorców wykonujących transport drogowy taksówką – zbiór tradycyjny**
19). **Stypendia szkolne i zasiłki szkolne – zbiór tradycyjny**

Rozdział V

Struktura zbioru danych osobowych.

§ 7

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi:

1). **Windykacja należności podatkowych –WIP – załącznik nr 1**
2). **Zbiór -rejestr ksiąg urodzeń, małżeństw i zgonów w USC – PB_USC - załącznik nr 2**
3). **Podatek od środków transportowych - POST - załącznik nr 3**
4). **Łączne zobowiązanie pieniężne - POGRUN – załącznik nr 4**
5). **Ewidencja ludności ELUD + - załącznik nr 5**
6). **Rejestr Wyborców WYB+ – załącznik nr 6**
7). **Ewidencja gruntów i budynków miasta i gminy Opatów – EWOPIS – załącznik nr 7**
8). **Ewidencja dowodów osobistych – System Wydawania Dowodów Osobistych – załącznik nr 8**

Rozdział V

Powiązania systemów w urzędzie.

§ 8

System WIP korzysta z bazy POGRUN oraz POST, oraz WYB+ korzysta z ELUD+ pozostałe systemy informatyczne używane w urzędzie działają niezależnie od siebie.

Rozdział VI

Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności danych przetwarzanych w systemie.

§ 9

Środki ochrony fizycznej

1). Urządzenia służące do przetwarzania danych osobowych znajdują się na I piętrze w pomieszczeniach zabezpieczonych zamkami patentowymi.
2). Kopie baz danych przechowywane są w kasie pancernej w pomieszczeniu nr 11A

§ 10

Środki sprzętowe, informatyczne i telekomunikacyjne.

1). Urządzenia wchodzące w skład systemu informatycznego podłączone są do odrębnego obwodu elektrycznego
2). Każdy z komputerów jest zabezpieczony UPS - em na wypadek zaniku napięcia albo awarii w sieci zasilającej.
3). Zastosowano sieć lokalną (Ethernet)
4). Kopie awaryjne wykonywane są na płytach CDR, CDR RW, DCD R, DVD RW.

§ 11

Środki ochrony w ramach oprogramowania systemu

1). Konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych jedynie za pośrednictwem aplikacji
2). System informatyczny pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu
3). Zastosowano działający w „tle" program antywirusowy na komputerach użytkowników
4). W systemie operacyjnym zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do sieci.

§ 12

Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych

1). Automatycznie rejestrowany jest identyfikator użytkownika wprowadzającego dane oraz datę pierwszego wprowadzenia tych danych
2). Zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji
3). Dla każdego użytkownika systemu jest ustalony odrębny identyfikator
4). Zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji

§ 13

Środki ochrony w ramach systemu użytkowego

Możliwość dostępu do danych osobowych, tylko po zalogowaniu się do sieci.

§ 14

Środki organizacyjne

1). Wyznaczono administratora bezpieczeństwa informacji: Jerzy Budzisz
2). Tymczasowe wydruki z danymi osobowymi są po ustaniu ich przydatności niszczone
3). Do obsługi systemu informatycznego dopuszczane są osoby na podstawie indywidualnego upoważnienia.
4). Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane są do zachowania ich w tajemnicy
5). Osoby upoważnione do przetwarzania danych osobowych są przed dopuszczeniem ich do tych danych szkolone w zakresie obwiązujących przepisów o ochronie danych osobowych.
6). Prowadzona jest ewidencja osób upoważnionych do przetwarzaniu danych osobowych
7). Ustalono instrukcję zarządzania systemem informatycznym
8). Zdefiniowano procedury postępowania w sytuacji:
naruszenia ochrony danych osobowych w postaci instrukcji,
9). Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

- likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
- przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
- naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

Rozdział VII
Postanowienia końcowe

§ 15

Polityka bezpieczeństwa przetwarzania danych osobowych wchodzi w życie z dniem jej wprowadzenia w Urzędzie Miasta i Gminy w Opatowie, określonym w Zarządzeniu Burmistrza Miasta i Gminy Opatów.

BURMISTRZ
mgr Krystyna Kielisz