ZARZĄDZENIE NR 243/2007
PREZYDENTA MIASTA KRAKOWA
Z DNIA 7 lutego 2007 roku

w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji Urzędu Miasta Krakowa.

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, z późn. zm.), § 10 zarządzenia Nr 18/2007 Prezydenta Miasta Krakowa z dnia 3 stycznia 2007 r., art. 36. ust 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. (Dz. U. 2002 r. Nr 101 poz. 926, z późn. zm.) oraz 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. 2004 r. Nr 100 poz. 1024), zarządza się, co następuje:

§1

1. Wprowadza się do stosowania Politykę Bezpieczeństwa Informacji Urzędu Miasta Krakowa, zwaną dalej Polityką Bezpieczeństwa.
2. Polityka Bezpieczeństwa, o której mowa w ust.1 stanowi załącznik do niniejszego Zarządzenia.

§ 2

Wykonanie zarządzenia powierza się Dyrektorowi Magistratu.

§ 3

Traci moc Uchwała Nr 752 /99 Zarządu Miasta Krakowa z dnia 12 lipca 1999 roku w sprawie dostosowania Systemu Informatycznego UMK do wymagań ustawy z dnia 29 sierpnia 1997 o ochronie danych osobowych.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

Prezydent Miasta Krakowa
/ - /

Załącznik do zarządzenia Nr 243/2007
Prezydenta Miasta Krakowa
z dnia 07.02.2007 r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI W URZĘDZIE MIASTA KRAKOWA
DOKUMENT GŁÓWNY

1. Zakres rozpowszechniania Polityki Bezpieczeństwa – dokument główny.

Niniejszy dokument powinien zostać rozpowszechniony wśród pracowników Urzędu Miasta Krakowa oraz może być rozpowszechniany bez żadnych ograniczeń poza Urzędem Miasta Krakowa.

2. Założenia i cele Polityki Bezpieczeństwa.

2.1 Cele.

Najważniejszym elementem każdej organizacji są jej pracownicy, czyli klienci wewnętrzni, ale nie należy zapominać o pozostałych zasobach, dzięki którym organizacja może sprawnie i bezpiecznie funkcjonować. W następnej kolejności po pracownikach a obok mienia, to właśnie informacja jest kolejnym z najważniejszych zasobów Urzędu Miasta Krakowa.

Ochrona pracowników oraz wszelkiego rodzaju mienia jest doskonale przez wszystkich rozumiana, akceptowana a przede wszystkim – opisana i usankcjonowana w wielu dokumentach, procedurach czy instrukcjach. Natomiast zbiór zasad dotyczących bezpieczeństwa informacji przetwarzanych w Magistracie jest rozproszony oraz niedostatecznie upowszechniony. A przecież to właśnie w znaczącym stopniu w oparciu o przetwarzane informacje sprawnie funkcjonuje Magistrat, a bezpieczeństwo tych informacji wpływa znacząco na reputację i gwarancje bezpieczeństwa w aspekcie prawnej odpowiedzialności Magistratu. Naruszenie bezpieczeństwa informacji (danych) kluczowych dla sprawnego funkcjonowania Urzędu, w tym także danych osobowych, mogłyby spowodować poważne następstwa prawne i ekonomiczne zarówno dla Urzędu jak również dla Gminy Miejskiej Kraków.

Zasady bezpieczeństwa informacji wymagają dokładnego określenia i muszą zostać poparte oraz wprowadzone przez najwyższe kierownictwo przedsiębiorstwa, co właśnie zostaje ujęte w niniejszej Polityce Bezpieczeństwa Informacji Urzędu Miasta Krakowa. Dokument ten wskazuje potrzebę ochrony informacji przetwarzanych w Magistracie jako wynikającą nie tylko z nakazów prawnych (jak np. Ustawa o ochronie danych osobowych), ale również z konieczności zagwarantowania sprawnego i bezpiecznego działania Urzędu. Określa również kierunek sprawnego wdrożenia takiej Polityki – głównie poprzez szkolenia i informowanie użytkowników systemów przetwarzania danych, ale także poprzez zaangażowanie pracowników Urzędu w proces tworzenia dokumentów szczegółowych.

2.2 Założenia ogólne.

W powszechnej świadomości funkcjonuje mylny pogląd, iż bezpieczeństwo informacji jest pojęciem związanym tylko z bezpieczeństwem teleinformatycznym oraz, że bezpieczeństwo takie jest zapewnione głównie poprzez ograniczenie dostępu do Internetu.

Z powyższego poglądu wypływają równie mylne wnioski, jak np. ten, że bezpieczeństwo informacji to sprawa tylko odpowiedniego sprzętu czy oprogramowania komputerowego a jako takie – pozostaje jedynie w gestii komórek informatycznych oraz jest niezwykle kosztowne. Natomiast większość norm związanych z bezpieczeństwem informacji podaje jako podstawę bezpieczeństwa informacji odpowiednią organizację zarządzania bezpieczeństwem – wskazanie osób odpowiedzialnych za poszczególne obszary bezpieczeństwa informacji oraz wskazanie jasnych i klarownych zasad postępowania dla użytkowników systemów przetwarzania informacji. A przede wszystkim – należy pamiętać o ewolucyjnym charakterze podejścia do zarządzania bezpieczeństwem, przy uwzględnieniu elementarnej zasady, która mówi, że niebezpieczeństwa nie można zlikwidować, można go tylko bardziej lub mniej znacząco zmniejszać.

Cykl zarządzania bezpieczeństwem informacji zgodnie z nowoczesnymi normami, czyli szerzej, niż określa to ustawa o ochronie danych osobowych, musi obejmować następujące kroki:

1. **Określenie zasobów,** czyli odpowiedź na pytanie: co trzeba chronić?
2. **Identyfikacja zagrożeń,** czyli odpowiedź na pytanie: przed czym/kim mamy to chronić?
3. **Określenie działań oraz środków zmniejszających zagrożenia,** czyli między innymi przygotowanie oraz wdrożenie polityki bezpieczeństwa.
4. **Przegląd skuteczności zastosowanych rozwiązań,** czyli między innymi przeprowadzanie okresowych audytów bezpieczeństwa.

Określenie zasobów informacyjnych Urzędu, które muszą być chronione, a więc określenie informacji, które należy chronić dla zagwarantowania sprawnego działania Urzędu oraz ze względu na wymogi prawne, a także zidentyfikowanie zagrożeń, jakie mogą oddziaływać na te informacje, pozwala na stworzenie **mapy zagrożeń**. Analiza taka pomaga określić:

- Jakie informacje (dane) Urząd posiada?
- Gdzie są one rozmieszczone?
- Jaki wpływ mają na funkcjonowanie Urzędu?
- Czy i jakie występują dla nich zagrożenia?
- Jakie jest prawdopodobieństwo utraty bądź zniszczenia tych danych?
- Które informacje muszą lub powinny być chronione, a które tego nie wymagają?
- Jakie działania w zakresie bezpieczeństwa są konieczne w celu zabezpieczenia chronionych informacji?

Na podstawie takiej mapy zagrożeń należy opracować szczegółowe polityki bezpieczeństwa informacji dla wszelkich systemów przetwarzania danych w Urzędzie.

Ponieważ bezpieczeństwo informacji przetwarzanych w Systemie Informatycznym jest zagadnieniem kluczowym dla całego bezpieczeństwa informacji w Magistracie, niezwykle istotna jest Polityka Bezpieczeństwa Systemu Informatycznego Urzędu, która powinna określać szczegółowe zasady bezpieczeństwa danych przetwarzanych w tym systemie. Polityka ta stworzy podstawy dla procedur, regulaminów, instrukcji, zasad zarządzania bezpieczeństwem Systemu Informatycznego oraz głównie na jej podstawie stworzony zostanie, drugi wymagany prawem dokument dotyczący bezpieczeństwa danych – Instrukcja Zarządzania Systemem Informatycznym UMK.

Ze względów na wskazane powyżej, strategiczne znaczenie Systemu Informatycznego dla przetwarzania danych w Urzędzie, niniejszy dokument w ostatnim rozdziale zawiera opis celów i zakres Polityki Bezpieczeństwa Systemu Informatycznego UMK i to właśnie tę Politykę należy opracować niezwłocznie w następnej kolejności.

2.3 Deklaracja Prezydenta Miasta Krakowa.

Niniejsza deklaracja została przygotowana w oparciu o polską normę (PN-ISO/IEC 17799), zgodnie z którą Polityka Bezpieczeństwa powinna zawierać oświadczenie o intencjach kierownictwa, potwierdzające cele i zasady bezpieczeństwa informacji:

DEKLARACJA PREZYDENTA MIASTA KRAKOWA

ZOBOWIĄZUJĘ SIĘ DO PODEJMOWANIA NIEZBĘDNYCH DZIAŁAŃ MAJĄCYCH NA CELU KOMPLEKSOWE ZABEZPIECZENIE INFORMACJI, JAKO ZASOBU PODLEGAJĄCEGO OCHRONIE PRAWNEJ I NIEZBĘDNEGO DO PRAWIDŁOWEGO ORAZ SPRAWNEGO FUNKCJONOWANIA URZĘDU MIASTA KRAKOWA.

PONADTO WYRAŻAM GOTOWOŚĆ PONIESIENIA KOSZTÓW ZWIĄZANYCH Z WDROŻENIEM I UTRZYMYWANIEM POLITYKI BEZPIECZEŃSTWA INFORMACJI.

KONSEKWENCJĄ NARUSZENIA ZASAD BEZPIECZEŃSTWA INFORMACJI SĄ KARY WYNIKAJĄCE Z USTAWY O OCHRONIE DANYCH OSOBOWYCH ORAZ KODEKSU PRACY.

Jacek Majchrowski

Prezydent Miasta Krakowa

W następstwie powyższej deklaracji, ustanawia się niniejszą Politykę Bezpieczeństwa Informacji Urzędu Miasta Krakowa oraz nakazuje się do wdrożenia i rozpowszechnienia tego dokumentu w UMK.

3. Zakres i podstawy normatywne Polityki Bezpieczeństwa.

Polityka Bezpieczeństwa Informacji powstała w związku z wykorzystywaniem danych osobowych w rozumieniu ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. 2002 r. Nr 101 poz. 926 z póź. zm.), a także innych danych krytycznych dla sprawnego funkcjonowania Urzędu oraz technologii informatycznych do realizacji zadań statutowych w Urzędzie Miasta Krakowa (zwanym dalej w skrócie UMK).

Niniejszy dokument stanowi najwyższej rangi dokument polityki bezpieczeństwa danych, w tym przede wszystkim danych osobowych w UMK, przetwarzanych we wszystkich systemach w UMK oraz jest on wiążący dla wszystkich komórek organizacyjnych Urzędu Miasta Krakowa, korzystających z tych systemów, a w szczególności Systemu Informatycznego UMK. Z systemów przetwarzania danych UMK mogą również korzystać inne podmioty gospodarcze nie ujęte powyżej na podstawie odrębnych umów, określających zasady korzystania z tych systemów, w szczególności ochronę dostępu do danych.

Na podstawie zawartych w tym dokumencie zasad bezpieczeństwa zostaną opracowane polityki szczegółowe, procedury, instrukcje i regulaminy.

Za opracowanie i wdrożenie tych dokumentów odpowiada powołany odrębnym zarządzeniem Zespół Zadaniowy ds. wdrożenia zasad ochrony informacji w Urzędzie Miasta Krakowa.

Powyższe szczegółowe dokumenty powstaną z wykorzystaniem doświadczeń praktycznych oraz treści zasad i zaleceń głównie poniższych aktów prawnych oraz pomocniczo – polskich norm (uwzględnionych również przy opracowywaniu niniejszej Polityki):

- Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. 2002 r. Nr 101 poz. 926 z póź. zm.).
- Rozporządzenie 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. 2004 r. Nr 100 poz. 1024).
- PN-13335-1: Technika Informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych.
- PN-ISO/IEC 17799: Technika Informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji.

4. Definicja informacji.

Na potrzeby zapisów niniejszej Polityki Bezpieczeństwa, przyjmuje się, iż reprezentacją informacji (danych) są wszelkie zapisy w formie papierowej, w układach elektronicznych oraz na innych nośnikach (np. magnetycznych czy optycznych), przetwarzane (zbierane, utrwalane, przechowywane, opracowywane, zmieniane, udostępniane i usuwane) w systemach komputerowych, papierowych i komunikacyjnych będących własnością Gminy Miejskiej Kraków i funkcjonujących w UMK, lub jedynie administrowanych przez UMK.

5. Własność informacji.

Wszelkie informacje przekazywane i przetwarzane w Urzędzie, nie oznaczone jako należące do osób trzecich, będą traktowane jako własność Urzędu.

Urząd chroni zarówno informacje własne jak i powierzone. Jest to podstawa do wszelkich dalszych regulacji dotyczących bezpieczeństwa informacji w Magistracie. Oznacza to, że informacje stanowiące własność Urzędu, nie mogą być zatajane wewnątrz Urzędu, (ale mogą być chronione, w tym także przed nieautoryzowanym dostępem), a wszelka korespondencja elektroniczna i papierowa, która została stworzona w obrębie Urzędu należy do UMK. Zabrania się używania wszelkich systemów przetwarzania informacji w Urzędzie do celów prywatnych, co w szczególności oznacza, że wszelka korespondencja (w tym także elektroniczna) jest własnością UMK.

6. Podział i ochrona informacji.

Wszystkie informacje w UMK są dzielone na chronione i nie chronione. Urząd zabezpiecza tylko informacje chronione. Bezpieczeństwo informacji jest rozumiane, jako jej:

- Poufność.
- Integralność.
- Dostępność.

Powyższa definicja bezpieczeństwa oznacza, iż informacje chronione w UMK muszą być zabezpieczane przed nieautoryzowanym dostępem, zmianą, utratą, uszkodzeniem, zniszczeniem lub zatajeniem.

Wszystkie informacje w UMK nie są domyślnie chronione, jeżeli nie zostały zidentyfikowane, opisane i oznaczone jako chronione. Założenie, że wszystkie informacje w Urzędzie są chronione, może powodować łamanie zasad bezpieczeństwa informacji przez pracowników Urzędu w celu wykonywania obowiązków służbowych lub do destabilizacji i paraliżu pracy w systemach przetwarzania informacji w UMK.

Osobą odpowiedzialną za identyfikację, opisanie i oznaczenie danych chronionych, przetwarzanych w Systemie Informatycznym UMK jest Administrator Informacji przetwarzanych w SI (powołany w rozdziale 7).

Osobą odpowiedzialną za identyfikację, opisanie i oznaczenie danych chronionych, przetwarzanych w pozostałych systemach w UMK jest Główny Administrator Danych (powołany w rozdziale 7).

Szczegółowe zasady bezpieczeństwa danych przetwarzanych w danym systemie, określają poszczególne polityki bezpieczeństwa informacji przetwarzanych w tych systemach opracowane przez Zespół Zadaniowy powołany osobnym zarządzeniem.

Informacje nie chronione, w razie potrzeby, mogą podlegać ochronie w ograniczonym zakresie (np. zabezpieczenie ogólnodostępnych informacji na stronie internetowej UMK jedynie przed ich nieautoryzowaną modyfikacją).

7. Powołanie osób odpowiedzialnych za zarządzanie bezpieczeństwem informacji w UMK.

1. W celu sprawnego zarządzania przetwarzaniem i bezpieczeństwem informacji, ustanawia się następujące funkcje i stanowiska:
   a. Funkcję **Głównego Administratora Informacji**, podległego bezpośrednio Prezydentowi Miasta Krakowa, upoważnionego do pełnienia funkcji Administratora Danych na zasadach i w zakresie określonym w ustawie o ochronie danych osobowych. Pełnienie tej funkcji powierza się Dyrektorowi Magistratu, który wykonuje ją przy pomocy Administratora Informacji przetwarzanych w SI, Administratora Informacji przetwarzanych poza SI oraz Administratora Bezpieczeństwa Informatycznego.
   b. Funkcję **Administratora Informacji przetwarzanych w SI**, podległego bezpośrednio Dyrektorowi Magistratu, upoważnionego do pełnienia funkcji Administratora Danych na zasadach i w zakresie określonym w ustawie o ochronie danych osobowych **w stosunku do danych osobowych przetwarzanych w Systemie Informatycznym UMK.** Pełnienie funkcji Administratora Informacji przetwarzanych w SI powierza się Dyrektorowi Wydziału Informatyki.
   c. Funkcję **Administratora Informacji przetwarzanych poza SI**, podległego bezpośrednio Dyrektorowi Magistratu, upoważnionego do pełnienia funkcji Administratora Danych na zasadach i w zakresie określonym w ustawie o ochronie danych osobowych **w stosunku do danych osobowych przetwarzanych poza SI**. Pełnienie funkcji Administratora Informacji przetwarzanych poza SI powierza się Z-cy Dyrektora Wydziału Organizacji i Nadzoru ds. Organizacyjnych.
   d. Stanowisko **Administratora Bezpieczeństwa Informatycznego**, podległego bezpośrednio Administratorowi Informacji przetwarzanych w SI UMK.
2. Administrator Informacji przetwarzanych poza SI jest odpowiedzialny za określenie celów i środków przetwarzania informacji, a w szczególności danych osobowych, we wszystkich systemach w UMK poza Systemem Informatycznym UMK. W tym:

a. Określenie jakiego rodzaju informacje są przetwarzane w UMK poza Systemem Informatycznym.
b. Ustalenie podziału informacji (określenie czy jest to informacja chroniona).
c. Określenie narzędzi, metod, miejsca i czasu przetwarzania informacji poza SI UMK.
d. Ustalenie własności informacji przetwarzanych poza SI UMK.
e. Przyznanie dostępu do informacji przetwarzanych poza SI UMK.
f. Określenie zasad bezpieczeństwa informacji chronionych przetwarzanych poza SI UMK.
g. Przygotowanie Polityki Bezpieczeństwa informacji chronionych przetwarzanych poza SI UMK oraz jej okresowe aktualizowanie.
h. Nadzór na przestrzeganiem zasad bezpieczeństwa informacji chronionych przetwarzanych poza SI UMK oraz nadzór nad przeprowadzaniem okresowych kontroli i audytów bezpieczeństwa informacji chronionych przetwarzanych poza SI UMK.

3. Administrator Informacji przetwarzanych w SI jest odpowiedzialny za określenie celu i środków przetwarzania informacji, a w szczególności danych osobowych, w Systemie Informatycznym UMK. W tym:
   a. Określenie jakiego rodzaju informacje są przetwarzane w SI UMK.
   b. Ustalenie podziału informacji (określenie czy jest to informacja chroniona).
   c. Określenie narzędzi, metod, miejsca i czasu przetwarzania informacji w SI UMK.
   d. Ustalenie własności informacji przetwarzanych w SI UMK.
   e. Przyznanie dostępu do informacji przetwarzanych w SI UMK oraz do samego SI UMK.
4. Administrator Bezpieczeństwa Informatycznego jest odpowiedzialny za:
   a. Określenie zasad bezpieczeństwa informacji chronionych przetwarzanych w SI UMK.
   b. Przygotowanie Polityki Bezpieczeństwa Systemu Informatycznego UMK oraz jej okresowe aktualizowanie.
   c. Zatwierdzanie, modyfikowanie i akceptację przed przedłożeniem do podpisu Prezydentowi lub Dyrektorowi Magistratu proponowanych zmian zasad i procedur bezpieczeństwa przygotowywanych w Oddziale Informatyki UMK.
   d. Określenie minimalnych wymagań bezpieczeństwa dla systemów i aplikacji przetwarzania informacji wchodzących w skład SI UMK oraz przyznawanie homologacji bezpieczeństwa dla systemów i aplikacji przeznaczonych do pracy w SI UMK.
   e. Nadzór nad przestrzeganiem zasad bezpieczeństwa informacji chronionych przetwarzanych w SI UMK.
   f. Przeprowadzanie okresowych kontroli i audytów bezpieczeństwa informacji chronionych przetwarzanych w SI UMK.

   Szczegółowy zakres odpowiedzialności i obowiązków Administratora Bezpieczeństwa Informatycznego został określony w osobnym Zarządzeniu Prezydenta Miasta Krakowa.

8. Wdrożenie Polityki Bezpieczeństwa.

Polityka bezpieczeństwa powinna być rozumiana, akceptowana a przede wszystkim przestrzegana przez wszystkich pracowników UMK. Ogłoszenie i wdrożenie polityki w odpowiedni sposób gwarantuje osiągnięcie powyższych celów – jednym z najważniejszych kroków są tutaj szkolenia pracowników w zakresie zasad bezpieczeństwa oraz włączenie pracowników na wczesnym etapie w tworzenie szczegółowych dokumentów polityki bezpieczeństwa. Zwłaszcza wspomniane wyżej szkolenia pracowników są niezwykle

istotnym etapem wdrożenia, albowiem są one gwarancją zrozumienia przez użytkowników (jakimi są głównie pracownicy UMK) systemów przetwarzania danych, zagrożeń i potrzeb zabezpieczania informacji. Pozwalają również podnieść ogólną kulturę ochrony informacji, a w konsekwencji – lepiej przygotować użytkowników systemów do wspierania polityki bezpieczeństwa w czasie przebiegu ich normalnej pracy.

Poza szkoleniami, obowiązkowym musi być również podpisywanie przez użytkowników systemów (głównie pracowników UMK) przed uzyskaniem dostępu do systemów przetwarzania informacji w UMK, oświadczeń o nieujawnianiu informacji - tzw. umów o poufności. Dodatkowo zobowiązanie do przestrzegania polityki bezpieczeństwa musi być umieszczone w zakresie obowiązków każdego pracownika UMK.

9. Zakres i cele Polityki Bezpieczeństwa Systemu Informatycznego UMK.

Zadania powierzane Systemowi Informatycznemu UMK (zwanemu dalej w skrócie SI UMK) są bardzo złożone i prócz tego, że zawierają w dużej części dane osobowe posiadają kluczowe znaczenie dla funkcjonowania Magistratu. Naturalnym, więc wydaje się wniosek, iż przetwarzanie danych w SI UMK, a zwłaszcza ich bezpieczeństwo wpływa znacząco na sprawność funkcjonowania Magistratu, trafność decyzji podejmowanych przez Prezydenta Miasta Krakowa oraz w zakresie ochrony danych osobowych – na reputację Magistratu i gwarancje bezpieczeństwa w aspekcie prawnej odpowiedzialności. Oczywiście w Urzędzie Miasta Krakowa dane osobowe są przetwarzane również poza Systemem Informatycznym, ale to właśnie w tym systemie przetwarza się je najczęściej i to właśnie on pozostaje kluczowym systemem przetwarzania wszystkich danych w Urzędzie.

Polityka Bezpieczeństwa Systemu Informatycznego UMK musi określać zasady ochrony informacji przetwarzanych w tym systemie, a więc musi mieć charakter ewolucyjny oraz zawierać (zgodnie z obowiązującym prawem) co najmniej:

a. Cel i zakres polityki bezpieczeństwa Systemu Informatycznego.
b. Zasady dostępu do informacji chronionych, przetwarzanych w SI.
c. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są informacje chronione w SI, a w szczególności dane osobowe.
d. Wykaz zbiorów informacji chronionych, (w szczególności danych osobowych) w SI UMK wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.
e. Opis struktury zbiorów danych (w szczególności danych osobowych oraz danych finansowych objętych wymaganiami Ustawy o Rachunkowości) wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.
f. Wykaz środków technicznych i organizacyjnych niezbędnych dla zapewnienia bezpieczeństwa informacji przetwarzanych w SI.
g. Sposób przepływu danych pomiędzy poszczególnymi systemami lub aplikacjami.
h. Wymagania dla aplikacji i systemów przetwarzania informacji chronionych.
i. Opis postępowania w przypadku wystąpienia sytuacji kryzysowych.
j. Obowiązki użytkowników informacji chronionych, w tym również obowiązki użytkowników uprzywilejowanych (administratorów).

W szczególności Polityka Bezpieczeństwa Systemu Informatycznego UMK powinna definiować rozwiązania programowe i sprzętowe, stosowane w SI w taki sposób, aby spełniały one wymogi określone w § 7 rozporządzenia 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, w tym szczególnie umożliwia uzyskanie informacji o odbiorcach w rozumieniu art. 7 pkt 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, którym dane osobowe zostały udostępnione oraz dacie i zakresie tego udostępnienia.

System Informatyczny UMK musi spełniać permanentnie wymagania w zakresie bezpieczeństwa właściwe co najmniej dla poziomu wysokiego, określonego w lit. C załącznika do 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. 2004 r. Nr 100 poz. 1024).

Opracowaniem i wdrożeniem Polityki Bezpieczeństwa Systemu Informatycznego UMK zajmie się powołany odrębnym zarządzeniem Zespół Zadaniowy ds. wdrożenia zasad ochrony informacji w Urzędzie Miasta Krakowa.