

**ZARZĄDZENIE NR 1536/2007**  
**PREZYDENTA MIASTA KRAKOWA**  
**Z DNIA 18 lipca 2007 roku**

**w sprawie wprowadzenia Instrukcji Zarządzania Systemem Informatycznym 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.), 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 Instrukcję Zarządzania Systemem Informatycznym Urzędu Miasta Krakowa, zwaną dalej Instrukcją Zarządzania SI UMK.
2. Instrukcja Zarządzania SI UMK, o której mowa w ust.1 stanowi załącznik do niniejszego Zarządzenia.

§ 2

Zarządzenie wchodzi w życie z dniem podpisania.

Prezydent Miasta Krakowa

/ - /



Załącznik do zarządzenia Nr 1536/2007  
Prezydenta Miasta Krakowa  
z dnia 18 lipca 2007 r.

**INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM  
URZĘDU MIASTA KRAKOWA**  
*(dokument szczegółowy Polityki Bezpieczeństwa Informacji UMK)*

**§ 1**

**Zakres rozpowszechniania**

Niniejszy dokument zostanie szeroko rozpowszechniony wśród pracowników Urzędu Miasta Krakowa oraz miejskich jednostek organizacyjnych będących użytkownikami Systemu Informatycznego UMK.

**§ 2**

**Cele i założenia**

Niniejsza instrukcja określa zasady zarządzania i użytkowania Systemem Informatycznym UMK, w tym:

1. definiuje podstawowe pojęcia oraz podział kompetencji i odpowiedzialności w odniesieniu do struktury organizacyjnej UMK,
2. określa zasady:
  - 1) korzystania i dostępu do Systemu Informatycznego UMK,
  - 2) korzystania ze sprzętu komputerowego w UMK,
  - 3) udostępniania danych chronionych przetwarzanych w Systemie Informatycznym UMK,
  - 4) rejestracji zbiorów danych osobowych.

**§ 3**

**Podstawy normatywne**

Instrukcja Zarządzania SI UMK powstała na podstawie dokumentu głównego Polityki Bezpieczeństwa Informacji UMK, w zgodzie z obowiązującymi przepisami prawa oraz ze szczególnym uwzględnieniem następujących dokumentów:

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

**§ 4**

**Definicje**

Ilekroć w niniejszym dokumencie jest mowa o:

1. *Systemie Informatycznym Urzędu Miasta Krakowa (SI UMK)* – rozumie się przez to zbiór, którym można zarządzać jako całością, składający się z wszystkich programów, narzędzi programowych, procedur przetwarzania informacji, urządzeń, przedmiotów (np. nośniki magnetyczne) oraz pomieszczeń (np. serwerownia), będących własnością Gminy Miejskiej Kraków i funkcjonujących w UMK lub administrowanych przez UMK, służących do przetwarzania informacji w postaci elektronicznej w UMK.
2. *Informacjach (danych)* – rozumie się przez to reprezentacje informacji (danych), czyli wszelkie zapisy w układach elektronicznych oraz na innych nośnikach (papierowych, magnetycznych, optycznych itp.) przetwarzane w SI UMK.
3. *Informacjach (danych) chronionych* – rozumie się przez to informacje (dane) przetwarzane w SI UMK, którym Urząd zapewnia bezpieczeństwo w rozumieniu definicji określonej w pkt.6.
4. *Danych osobowych* – rozumie się przez to dane (informacje) osobowe w rozumieniu ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. (Dz. U. 2002 r. Nr 101 poz. 926, z późn. zm.).
5. *Przetwarzaniu informacji* – rozumie się przez to jakiegokolwiek operacje wykonywane na informacji, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, wykonywane w SI UMK.
6. *Bezpieczeństwie informacji* – rozumie się przez to zapewnienie poufności, integralności i dostępności informacji przetwarzanych w SI UMK, czyli zabezpieczane jej przed nieautoryzowanym dostępem, zmianą, utratą, uszkodzeniem, zniszczeniem lub zatajeniem. UMK zabezpiecza tylko informacje chronione, czyli takie, które zostały zidentyfikowane, opisane i oznaczone jako chronione, zgodnie z Polityką Bezpieczeństwa UMK.
7. *Poufności informacji* – rozumie się przez to właściwość zapewniającą, że informacja przetwarzana w SI UMK jest udostępniana tylko osobom upoważnionym.
8. *Integralności informacji* – rozumie się przez to właściwość zapewniającą, że informacja przetwarzana w SI UMK nie została zmieniona lub zniszczona w sposób nieautoryzowany, czyli, że została zachowana dokładność i kompletność informacji.
9. *Dostępności informacji* – rozumie się przez to właściwość zapewniającą, że informacja przetwarzana w SI UMK jest dostępna dla osób upoważnionych zawsze wtedy, gdy jest to potrzebne.
10. *Zbiorze danych* – rozumie się przez to każdy posiadający strukturę zestaw danych (informacji) przetwarzanych w SI UMK, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
11. *Aplikacji* – rozumie się przez to program komputerowy, będący częścią SI UMK oraz przetwarzający informacje.
12. *Oprogramowaniu systemowym* – rozumie się przez to systemy operacyjne, bazodanowe lub inne programy, niezbędne do uruchomienia oraz eksploatacji aplikacji.
13. *Urządzeniu komputerowym* – rozumie się przez to każde urządzenie elektroniczne służące do przetwarzania oraz teletransmisji informacji, np. komputer, serwer, urządzenie sieciowe, drukarka, skaner, itp.
14. *Sieci komputerowej* – rozumie się przez to okablowanie, urządzenia komputerowe oraz oprogramowanie służące do teletransmisji informacji.
15. *Błędzie* – rozumie się przez to każde nieprawidłowe działanie aplikacji, oprogramowania systemowego, urządzeń komputerowych, sieci komputerowej lub innych elementów SI UMK niezgodne z instrukcją użytkownika lub dokumentacją

- techniczną.
16. *Administratorze Informacji przetwarzanych w SI* – rozumie się przez to dyrektora wydziału właściwego dla spraw informatycznych, osobę upoważnioną do pełnienia funkcji Administratora Danych na zasadach i w zakresie określonym w ustawie o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. 2002 r. Nr 101 poz. 926 z póź. zm.) w stosunku do danych osobowych przetwarzanych w Systemie Informatycznym UMK.
  17. *Merytorycznym Administratorze Informacji* – rozumie się przez to dyrektora wydziału właściwego dla danego zakresu danych, osobę odpowiedzialną merytorycznie za przetwarzanie informacji oraz w dyspozycji, której znajdują się te informacje.
  18. *Administratorze Systemu* – rozumie się przez to kierownika referatu w wydziale właściwym do spraw informatycznych, osobę odpowiedzialną za ciągłość pracy, rozwój oraz bezpieczeństwo Systemu Informatycznego UMK, w tym za techniczne przetwarzanie informacji w Systemie Informatycznym UMK oraz za bezpieczeństwo tych informacji.
  19. *Administratorze Bezpieczeństwa Informatycznego* – rozumie się przez to osobę odpowiedzialną za nadzór nad bezpieczeństwem informacji przetwarzanych w SI UMK.
  20. *Administratorze Technicznym* – rozumie się przez to pracownika wydziału właściwego do spraw informatycznych, osobę odpowiedzialną za techniczny nadzór nad pracą aplikacji, oprogramowania systemowego, sieci komputerowej lub urządzeń komputerowych.
  21. *Gospodarzu* – rozumie się przez to pracownika wydziału właściwego dla danego zakresu danych, osobę odpowiedzialną za merytoryczny nadzór nad pracą aplikacji.
  22. *Koordinatorze* – rozumie się przez to osobę odpowiedzialną za merytoryczny nadzór nad pracą grupy aplikacji obsługujących spójny obszar merytoryczny .
  23. *Użytkownika* – rozumie się przez to uprawnioną osobę, która uzyskała dostęp i korzysta z zasobów SI UMK oraz może uzyskać dostęp do informacji chronionych przetwarzanych w SI UMK.
  24. *Identyfikatorze użytkownika* – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę, która jest użytkownikiem SI UMK.
  25. *Hasła* – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych wykorzystywany w procesie uwierzytelniania użytkownika przy uzyskiwaniu dostępu do SI UMK i znany jedynie użytkownikowi.
  26. *Uwierzytelnianiu* – rozumie się przez to proces identyfikacji użytkownika, czyli ustalenie jego tożsamości na podstawie podanego identyfikatora użytkownika oraz hasła.
  27. *Autoryzacji* – rozumie się przez to proces weryfikujący, czy dany użytkownik (o ustalonej w procesie uwierzytelniania tożsamości) ma prawo dostępu do informacji (danych), do których usiłuje uzyskać dostęp.

## **§ 5 Przepisy ogólne**

1. Postanowienia niniejszej Instrukcji są wiążące dla wszystkich komórek organizacyjnych UMK oraz miejskich jednostek organizacyjnych , korzystających z SI UMK.
2. Postanowienia niniejszej instrukcji są wiążące dla wszystkich osób, nie będących pracownikami UMK i miejskich jednostek organizacyjnych, które otrzymały dostęp

- do SI UMK.
3. Z Systemu Informatycznego UMK mogą również korzystać inne podmioty nie ujęte w ust. 1 na podstawie odrębnej umowy, określającej zasady korzystania z SI UMK, w szczególności ochronę dostępu do danych chronionych.
  4. W karcie obiegowej pracownika wprowadza się pozycję w brzmieniu „Administrator Systemu pok. 50, Plac Wszystkich Świętych 3-4”.
    - 1) Administrator Systemu, który jest odpowiedzialny za prowadzenie ewidencji użytkowników SI UMK lub osoba przez niego upoważniona, ma obowiązek potwierdzić na karcie obiegowej wyrejestrowanie identyfikatora użytkownika lub jego brak.
    - 2) Obowiązek uzyskania potwierdzenia wyrejestrowania identyfikatora lub jego braku dotyczy wszystkich pracowników UMK, którym ustał stosunek pracy.
  5. Administrator Informacji przetwarzanych w SI bierze w zarząd wszystkie urządzenia komputerowe będące na stanie Urzędu Miasta Krakowa. W szczególności dotyczy to uprawnień do:
    - 1) rozdziału nowo zakupionych urządzeń komputerowych,
    - 2) zmian w konfiguracji sieci komputerowej, urządzeń komputerowych, oprogramowania systemowego, aplikacji oraz podsystemów.
  6. Funkcję Administratora Informacji przetwarzanych w SI pełni Dyrektor Wydziału Informatyki na podstawie odrębnego zarządzenia Prezydenta Miasta Krakowa. Zakres odpowiedzialności i kompetencji Administratora Informacji przetwarzanych w SI określa załącznik nr 1 do Instrukcji.
  7. Merytorycznym Administratorem Informacji jest osoba odpowiedzialna merytorycznie za przetwarzanie określonych grup informacji w SI UMK. W przypadku niemożności ustalenia dla określonej grupy danych Merytorycznego Administratora Informacji, osobą merytorycznie odpowiedzialną za te dane jest Administrator Informacji przetwarzanych w SI. Zakres odpowiedzialności i kompetencji Merytorycznego Administratora Informacji określa załącznik nr 1 do Instrukcji.
  8. Administratora Systemu powołuje Administrator Informacji przetwarzanych w SI UMK. Zakres odpowiedzialności i kompetencji Administratora Systemu określa załącznik nr 1 do Instrukcji. Administrator Systemu kieruje pracą Administratorów Technicznych.
  9. Administratora Bezpieczeństwa Informatycznego powołuje Dyrektor Magistratu. Zakres odpowiedzialności i kompetencji Administratora Bezpieczeństwa Informatycznego określa odrębne zarządzenie prezydenta miasta..
  10. Administratora Technicznego powołuje Administrator Informacji przetwarzanych w SI UMK. Zakres odpowiedzialności i kompetencji Administratora Technicznego określa załącznik nr 1.
  11. Gospodarza powołuje Merytoryczny Administrator Informacji, natomiast Koordynatora powołuje Dyrektor Magistratu. Zakres odpowiedzialności i kompetencji Gospodarza i Koordynatora określa załącznik nr 1.
  12. Zakres odpowiedzialności i kompetencji użytkownika określa załącznik nr 1.

## **§ 6**

### **Zasady dostępu i korzystania z SI UMK**

1. Zasady dostępu i korzystania z SI UMK określają regulaminy:
  - a) korzystania z SI UMK, stanowiący załącznik nr 2,
  - b) korzystania z urządzeń komputerowych UMK, stanowiący załącznik nr 3,

- c) wdrażania i eksploatacji aplikacji, stanowiący załącznik nr 4,
  - d) udostępniania danych oraz rejestracji zbiorów danych osobowych, stanowiący załącznik nr 5,
  - e) przyznawania dostępu do SI UMK, stanowiący załącznik nr 6,
2. Każda osoba przed uzyskaniem identyfikatora użytkownika oraz każdy użytkownik SI UMK zobowiązany jest podpisać oświadczenie o zachowaniu poufności, którego formularz stanowi załącznik nr 7.

## **Role i odpowiedzialności w SI UMK**

### **I. ADMINISTRATOR INFORMACJI PRZETWARZANYCH W SI**

Administrator Informacji przetwarzanych w SI jest odpowiedzialny za:

1. Zarządzanie SI UMK.
2. Określenie jakiego rodzaju informacje są przetwarzane w SI UMK, w stosunku do informacji, co do których nie można wskazać Merytorycznego Administratora Informacji.
3. Ustalenie podziału informacji (informacja chroniona/niechroniona), w stosunku do informacji, co do których nie można wskazać Merytorycznego Administratora Informacji
4. Określenie narzędzi, metod, miejsca i czasu przetwarzania danych osobowych w SI UMK oraz pozostałych informacji chronionych, co do których nie można wskazać Merytorycznego Administratora Informacji.
5. Wyraża zgodę na przyznanie dostępu oraz zmiany uprawnień do danych osobowych przetwarzanych w SI UMK oraz do pozostałych informacji chronionych, co do których nie można wskazać Merytorycznego Administratora Informacji, a także do samego SI UMK.
6. Poprawność merytoryczną danych chronionych przetwarzanych w SI UMK co do których nie można wskazać Merytorycznego Administratora Informacji.
7. Zgodność merytoryczną aplikacji przetwarzających informacje chronione, co do których nie można wskazać Merytorycznego Administratora Informacji, z obowiązującymi aktami prawnymi.
8. Rejestrację zbiorów danych w Generalnym Inspektoracie Ochrony Danych Osobowych, jeżeli są one częścią SI UMK oraz zawierają dane osobowe.
9. Zastosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych w SI UMK informacji chronionych, a w szczególności za zabezpieczenie tych danych przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieupoważnioną, uszkodzeniem lub zniszczeniem.
10. Określenie budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są informacje chronione w SI UMK.
11. Zabezpieczenie obszarów określonych w ust. 10 w sposób uniemożliwiający dostęp do nich osób nieupoważnionych.
12. Nadzór nad prowadzeniem bieżącej ewidencji wszystkich użytkowników SI UMK.
13. Udzielanie zgody na udostępnianie danych osobowych zgodnie z ustawą o ochronie danych osobowych oraz pozostałych informacji chronionych, co do których nie można wskazać Merytorycznego Administratora Informacji – zgodnie z obowiązującymi przepisami prawa.
14. Udzielanie zgody na zakładanie zbiorów danych zawierających dane osobowe lub pozostałe informacje chronione, na lokalnych lub przenośnych urządzeniach komputerowych (komputery typu PC lub laptopy) oraz ewidencjonowanie tych zbiorów.
15. Zatwierdzanie instrukcji postępowania oraz procedur dla SI UMK.



## **II. MERYTORYCZNY ADMINISTRATOR INFORMACJI**

Funkcję Merytorycznego Administratora Informacji pełni kierujący komórką organizacyjną, odpowiadający merytorycznie za określoną grupę informacji. Wskazanie merytorycznie odpowiedniej komórki organizacyjnej następuje za pomocą odrębnych zarządzeń Prezydenta Miasta Krakowa. Merytoryczny Administrator Informacji w stosunku do danych, którymi merytorycznie zarządza, jest odpowiedzialny za:

1. Określenie jakiego rodzaju informacje są przetwarzane w SI UMK.
2. Ustalenie podziału informacji (informacja chroniona/niechroniona).
3. Określenie narzędzi, metod, miejsca i czasu przetwarzania informacji chronionych w SI UMK.
4. Wyrażanie zgody na przyznanie dostępu oraz zmiany uprawnień do informacji chronionych przetwarzanych w SI UMK.
5. Poprawność merytoryczną danych chronionych przetwarzanych w SI UMK.
6. Zgodność merytoryczną aplikacji przetwarzających informacje chronione z obowiązującymi aktami prawnymi.
7. Udzielanie zgody na udostępnianie informacji chronionych zgodnie z obowiązującymi przepisami prawa.
8. Zapewnienie przeszkolenia użytkowników przez Gospodarza w zakresie prawidłowego korzystania z aplikacji zgodnie z powierzonymi im obowiązkami.
9. Powołanie Gospodarza aplikacji.

## **III. ADMINISTRATOR SYSTEMU**

Funkcję Administratora Systemu w stosunku do odpowiedniego obszaru zasobów SI UMK pełni Kierownik Referatu w Wydziale Informatyki odpowiadającego merytorycznie za dany obszar (aplikacje, oprogramowanie systemowe, sieci komputerowe lub urządzenia komputerowe). Wskazanie merytorycznie odpowiedniego Referatu następuje za pomocą zarządzenia Prezydenta Miasta Krakowa (w sprawie podziału na wewnętrzne komórki organizacyjne oraz szczegółowego zakresu działania Wydziału Informatyki). Administrator Systemu w stosunku do obszaru SI UMK, którym merytorycznie administruje, jest odpowiedzialny za:

1. Koordynację działań zapewniających sprawne funkcjonowanie, zabezpieczenie SI UMK przed niepowołanym dostępem oraz techniczne zapewnienie Bezpieczeństwa Informacji chronionych.
2. Opracowanie instrukcji postępowania na wypadek awarii urządzeń komputerowych, oprogramowania systemowego, aplikacji oraz sieci komputerowej.
3. Prowadzenie bieżącej ewidencji użytkowników SI UMK.
4. Ewidencjonowanie udostępniania danych osobowych zgodnie z ustawą o ochronie danych osobowych.
5. Określenie rodzaju aplikacji oraz urządzeń komputerowych, które są niezbędne do realizacji zadań jednostek organizacyjnych UMK, a także opiniowanie aplikacji i urządzeń zaproponowanych przez merytoryczne jednostki organizacyjne UMK.
6. Administrowanie serwisem urządzeń komputerowych, oprogramowaniem systemowym, aplikacjami, siecią komputerową SI UMK.
7. Zapewnienie bezpieczeństwa informacji chronionych przetwarzanych na indywidualnych urządzeniach komputerowych użytkowników SI UMK.
8. Obsługę i organizację techniczną dostępu do usług SI UMK.
9. Rozbudowę SI UMK oraz wprowadzanie nowych technologii.
10. Opiniowanie instrukcji postępowania oraz procedur przygotowanych przez

odpowiedniego Administratora Technicznego określających zarządzanie Systemem Informatycznym UMK.

11. Wdrażanie aplikacji w SI UMK oraz zapewnienie ciągłości ich pracy ze strony technicznej.
12. Wskazywanie norm i standardów dotyczących urządzeń komputerowych, sieci komputerowej, Oprogramowania Systemowego oraz aplikacji będących częścią SI UMK.
13. Prowadzenie zakupów urządzeń komputerowych, aplikacji oraz Oprogramowania Systemowego przeznaczonych do wdrożenia w SI UMK.
14. Koordynowanie Asysty Technicznej dla urządzeń komputerowych, aplikacji oraz Oprogramowania Systemowego będących częścią SI UMK.

#### **IV. ADMINISTRATOR TECHNICZNY**

Funkcję Administratora Technicznego w stosunku do odpowiednich elementów SI UMK pełni odpowiedni pracownik referatu w Wydziale Informatyki, odpowiadający merytorycznie za te elementy. Administrator Techniczny w stosunku do elementów SI UMK (Aplikacje, Oprogramowanie Systemowe, sieci komputerowe lub urządzenia komputerowe), którymi merytorycznie administruje, jest odpowiedzialny za:

1. Konfigurację i administrację odpowiednich elementów SI UMK, w tym także w stopniu zapewniającym Bezpieczeństwo Informacji.
2. Bieżące monitorowanie odpowiednich elementów SI UMK, w tym także pod kątem prób nieautoryzowanego dostępu do Informacji Chronionych.
3. Przeciwdziałanie próbom włamania, zniszczenia oraz nieautoryzowanego dostępu do odpowiednich elementów SI UMK, w tym także do informacji chronionych.
4. Techniczne udostępnianie informacji chronionych, za zgodą Administratora Informacji przetwarzanych w SI lub odpowiedniego Merytorycznego Administratora Informacji, jeżeli użytkownik nie ma uprawnień bądź możliwości.
5. Opracowanie procedur określających zarządzanie odpowiednimi elementami SI UMK.
6. Tworzenie kopii awaryjnych danych chronionych z wyłączeniem danych przetwarzanych na lokalnych urządzeniach komputerowych oraz zasobów lub konfiguracji odpowiednich elementów SI UMK, niezbędnych do prawidłowej pracy SI UMK lub do przetwarzania danych chronionych.
7. Zabezpieczenie kopii awaryjnych, określonych w ust.6 i opracowanie procedur określających sposób ich tworzenia, przechowywania i odtwarzania.
8. Prowadzenie systemu kont użytkowników odpowiednich elementów SI UMK.
9. Umożliwienie archiwizowania danych chronionych przetwarzanych na lokalnych urządzeniach komputerowych (komputery typu PC lub laptopy) użytkowników.
10. Prowadzenie asysty technicznej dla odpowiednich elementów SI UMK oraz analizowanie i przedstawianie błędów zgłaszanych przez użytkowników partnerom zewnętrznym (wykonawca aplikacji lub serwis zewnętrzny).
11. Prowadzenie dokumentacji technicznej dotyczącej odpowiednich elementów SI UMK.
12. Przeprowadzanie analiz oraz proponowanie rozwiązań dotyczących rozwoju, integracji i współpracy z innymi odpowiednimi elementami SI UMK.
13. Administrowanie uprawnieniami użytkowników do odpowiednich elementów SI UMK, w tym także przy współpracy z Gospodarzami aplikacji.
14. Administrowanie licencjami do odpowiednich elementów SI UMK.
15. Współpracę z jednostkami organizacyjnymi UMK przy tworzeniu i ochronie lokalnych zbiorów danych chronionych oraz przy przejmowaniu danych z innych aplikacji lub zbiorów danych nie będących elementami SI UMK.

16. Koordynacja prawidłowej eksploatacji odpowiednich elementów SI UMK przez użytkowników.

## V. GOSPODARZ i KOORDYNATOR

1. Funkcję Gospodarza pełni pracownik komórki organizacyjnej UMK na prawach Wydziału, merytorycznie odpowiedzialnej za przetwarzanie odpowiedniego zakresu danych. Gospodarz, w stosunku do odpowiedniego zakresu danych jest odpowiedzialny za:
  - a) Merytoryczna koordynacja nad przetwarzaniem danych przez użytkowników SI UMK,
  - b) kontrolowanie i wypełnianie zbiorów danych będących słownikami aplikacji.
  - c) prowadzenie szkoleń dla nowych użytkowników aplikacji (przy współpracy Administratora Technicznego),
  - d) opracowywanie dla użytkowników regulaminów, instrukcji oraz procedur korzystania z aplikacji,
  - e) gromadzenie uwag merytorycznych i technicznych o pracy aplikacji i przekazywanie ich odpowiedniemu Koordynatorowi lub Administratorowi Technicznemu,
  - f) wnioskowanie do Koordynatora lub Administratora Technicznego o dokonanie zmian w aplikacji usprawniających pracę użytkowników,
  - g) wnioskowanie do Koordynatora lub Administratora Technicznego o dostosowanie aplikacji do zmian w obowiązujących aktach prawnych oraz strukturze organizacyjnej UMK,
  - h) informowanie Administratora Technicznego o niewłaściwym wprowadzeniu przez użytkownika danych powodujących błędne działanie aplikacji lub aplikacji z nim powiązanych,
  - i) wnioskowanie do Administratora Informacji przetwarzanych w SI lub odpowiedniego Merytorycznego Administratora Informacji o cofnięcie uprawnień użytkownikowi, który wykorzystał je w sposób niewłaściwy,
2. Funkcję Koordynatora pełni pracownik komórki organizacyjnej UMK na prawach Wydziału, odpowiedzialny za merytoryczny nadzór nad pracą grupy aplikacji obsługujących spójny obszar merytoryczny (np. obszar finansowy, obszar MSIP itp.). Koordynatora powołuje się do pewnych określonych obszarów działania o zasięgu ponad wydziałowym). Koordynator w stosunku do określonego obszaru danych jest odpowiedzialny za:
  - a) koordynację i kontrolę poprawności działań mających na celu stworzenie spójnej, zintegrowanej bazy danych, opracowywanie zasad powiązania ze sobą poszczególnych aplikacji przetwarzających odpowiedni obszar danych i przepływu danych między aplikacjami,
  - b) kierowanie pracami wdrożeniowymi w poszczególnych wydziałach obsługujących odpowiedni obszar danych,
  - c) bieżące monitorowanie działania zintegrowanego obszaru danych oraz analiza potrzeb i oczekiwań decydentów i użytkowników w tym obszarze,
  - d) współpraca z Administratorem Informacji przetwarzanych w SI oraz z odpowiednim Merytorycznym Administratorem Informacji, Gospodarzem i Administratorem Technicznym, uczestnictwo w naradach koordynacyjnych w celu omówienia istniejących nieprawidłowości oraz koniecznych modyfikacji w Aplikacjach,
  - e) opracowywanie założeń do modyfikacji i modernizacji aplikacji,

- f) wnioskowanie do odpowiedniego Administratora Technicznego o dostosowanie aplikacji do zmian w obowiązujących aktach prawnych, procedurach oraz strukturze organizacyjnej UMK,
- g) organizowanie szkoleń Gospodarzy poszczególnych aplikacji oraz szkoleń i prezentacji dla decydentów z zakresu funkcjonowania zintegrowanego obszaru danych,
- h) kontrolowanie i nadzorowanie wypełniania zbiorów danych będących wspólnymi słownikami aplikacji wchodzących w skład koordynowanego obszaru,
- i) weryfikacja wraz z odpowiednim Administratorem Technicznym przekazanych przez Gospodarzy uwag merytorycznych o pracy aplikacji oraz wnioskowanie o modyfikacje aplikacji,
- j) opracowywanie regulaminów, instrukcji dla użytkowników oraz procedur korzystania z aplikacji,
- k) opiniowanie każdorazowo zakupu nowej aplikacji z danego zakresu.

## VI. UŻYTKOWNIK

1. Użytkownikiem jest każda osoba, która uzyskała dostęp do SI UMK.
2. Użytkownikami o specjalnych uprawnieniach są wszyscy Administratorzy, Gospodarze i Koordynatorzy.
3. Użytkownik jest odpowiedzialny za:
  - a) niezwłoczne poinformowanie bezpośredniego przełożonego oraz Administratora Technicznego o nieautoryzowanym dostępie do informacji chronionych,
  - b) zachowanie w tajemnicy wszelkich posiadanych haseł chroniących jego konta użytkownika w SI UMK,
  - c) zmianę haseł do posiadanych kont użytkownika, co najmniej raz na miesiąc,
  - d) wykorzystywanie posiadanych identyfikatorów użytkownika wyłącznie do zadań związanych z pełnionym stanowiskiem,
  - e) uzyskanie zgody Administratora Informacji przetwarzanych w SI na zakładanie zbiorów danych zawierających informacje chronione, na lokalnych lub przenośnych urządzeniach komputerowych (komputery typu PC lub laptopy),
  - f) tworzenie kopii awaryjnych (archiwizację) Informacji Chronionych, przetwarzanych na lokalnych lub przenośnych urządzeniach komputerowych (komputery typu PC lub laptopy),
  - g) zapewnienie bezpieczeństwa informacji chronionych przetwarzanych na lokalnych lub przenośnych urządzeniach komputerowych (komputery typu PC lub laptopy),
  - h) prawidłowe korzystanie z aplikacji zgodnie z powierzonymi obowiązkami służbowymi,
  - i) bieżącą ochronę przed wirusami komputerowymi lokalnego urządzenia komputerowego stanowiącego jego stanowisko pracy,
  - j) urządzenia komputerowe przekazane mu do eksploatacji,
  - k) zgłaszanie awarii urządzeń komputerowych, oprogramowania systemowego, sieci komputerowej odpowiedniemu Administratorowi Technicznemu,
  - l) informowanie Gospodarza lub odpowiedniego Administratora Systemu o wszelkich nieprawidłowościach działania aplikacji,
  - m) zgłaszanie Gospodarzowi wszelkich zauważonych nieprawidłowości danych przetwarzanych w aplikacji,
  - n) zachowanie szczególnej staranności przy przetwarzaniu danych, aby dane te były:
    - przetwarzane zgodnie z prawem,
    - zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
    - merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.

## **Regulamin korzystania z SI UMK**

### **§ 1 Przepisy ogólne**

1. System Informatyczny Urzędu Miasta Krakowa, zwany dalej SI UMK, służy do przetwarzania informacji w UMK w postaci elektronicznej, wspomagając zarządzanie Gminą Miejską Kraków w zakresie administracji samorządowej.
2. System Informatyczny UMK tworzą poniższe elementy, będące własnością Gminy Kraków i funkcjonujące w UMK lub administrowane przez UMK:
  - a) Aplikacje oraz Oprogramowanie Systemowe,
  - b) zarządzenia, regulaminy, polityki i instrukcje dotyczące zarządzania, administrowania, używania i udostępniania samego SI UMK oraz informacji w nim przetwarzanych,
  - c) Sieć komputerowa i urządzenia komputerowe,
  - d) pozostałe przedmioty i urządzenia służące do wspomagania pracy sieci i urządzeń komputerowych lub do przetwarzania danych w SI UMK, (np. nośniki danych),
  - e) pomieszczenia służące do przetwarzania informacji w SI UMK (np. serwerownia lub węzły sieciowe).
3. Zabrania się używania SI UMK do celów prywatnych, co w szczególności oznacza, że wszelkie dane przetwarzane w SI UMK nie oznaczone jako własność osób trzecich, są własnością UMK – w tym także korespondencja elektroniczna.
4. Zabrania się uruchamiania w SI UMK urządzeń komputerowych nie będących własnością Gminy Miejskiej Kraków lub nie administrowanych przez UMK, w tym komputerów prywatnych lub urządzeń służących do teletransmisji danych.
5. Systemem Informatycznym UMK zarządza Administrator Informacji przetwarzanych w SI.
6. Z SI UMK mogą korzystać wyłącznie uprawnieni i zarejestrowani w Systemie Użytkownicy.
7. Wszelkie osoby korzystające z SI UMK są zobowiązane do przestrzegania prawa, zasad współżycia społecznego oraz zasad etyki. Zabrania się podejmowania działań, które naruszałyby dobra osobiste innych osób lub narażały te osoby na straty moralne lub materialne.
8. Wszelkie osoby, które z racji korzystania lub administrowania Systemem Informatycznym UMK mają lub mogą uzyskać dostęp do służbowych i osobistych danych innych użytkowników SI UMK zobowiązane są do zachowania ich w tajemnicy.
9. Wobec osób naruszających zasady określone w §1 pkt 7, zostanie wszczęte postępowanie wynikające z odpowiednich przepisów o odpowiedzialności służbowej, dyscyplinarnej, cywilnej lub karnej.

### **§ 2 Konto użytkownika w Systemie Informatycznym**

1. Dla każdego użytkownika SI UMK Administrator Systemu lub Administrator Techniczny ustala odrębny identyfikator użytkownika.
2. Każdy użytkownik SI UMK może posiadać tylko jeden identyfikator użytkownika taki

- sam dla wszystkich posiadanych kont w SI UMK oraz nie można zmieniać tego identyfikatora lub przyznawać takiego samego identyfikatora innemu użytkownikowi.
3. Administrator Systemu oraz Administrator Techniczny może posiadać więcej niż jeden identyfikator, pod warunkiem, iż żaden z używanych przez niego identyfikatorów użytkownika nie jest używany przez innego użytkownika SI UMK (w tym także innego Administratora).
  4. Odpowiedni Administrator Systemu prowadzi ewidencję wszystkich przyznanych identyfikatorów użytkownika w SI UMK (w tym także Administratorów). Ewidencja powyższa ma charakter informacji chronionych.
  5. Każdy pracownik UMK ma prawo do posiadania konta użytkownika w SI UMK, umożliwiającego mu korzystanie z poczty elektronicznej UMK. Konto to jest tworzone na wniosek bezpośredniego przełożonego pracownika.
  6. Konto w aplikacji przetwarzającej informacje chronione jest tworzone na wniosek bezpośredniego przełożonego użytkownika lub samego użytkownika po uzyskaniu akceptacji odpowiedniego Merytorycznego Administratora Informacji lub Administratora Informacji przetwarzanych w SI.
  7. Konta w pozostałych Aplikacjach są tworzone na wniosek bezpośredniego przełożonego użytkownika lub samego użytkownika.
  8. Wszelkie konta użytkownika w całym SI UMK zakłada odpowiedni Administrator Techniczny, który powiadamia o tym fakcie osoby wnioskujące.
  9. Konto użytkownika może być wykorzystywane przez użytkownika wyłącznie do zadań związanych z pełnionym stanowiskiem. W szczególności nie może być ono wykorzystywane do rozpowszechniania treści i obrazów wulgarnych, obrażających osoby trzecie, naruszających czyjekolwiek dobra osobiste lub niezgodnych z prawem.
  10. Hasło użytkownika musi składać się co najmniej z 8 znaków, w tym co najmniej z jednej dużej litery, jednej małej litery, jednej cyfry i jednego znaku nie będącego literą ani cyfrą.
  11. Hasło użytkownika musi być zmieniane raz na miesiąc.
  12. Osobą odpowiedzialną za zmianę hasła jest użytkownik.
  13. W przypadku utraty hasła użytkownik zobowiązany zgłosić się niezwłocznie do odpowiedniego Administratora Technicznego.
  14. Hasła użytkownika utrzymuje się w tajemnicy, również po upływie ich ważności.
  15. Administrator Techniczny ma prawo, zablokować konto użytkownika, który niewłaściwie chroni swoje hasło do czasu zmiany hasła na spełniające wymogi bezpieczeństwa.
  16. Konto użytkownika wykorzystywane niezgodnie z postanowieniami niniejszej instrukcji jest blokowane. O tym fakcie informowany jest przełożony użytkownika. Po uzgodnieniu z Administratorem Technicznym konto jest odblokowywane lub usuwane.
  17. Każdy użytkownik SI UMK jest zobowiązany do podpisania *Oświadczenia o zachowaniu poufności*, którego wzór został określony w załączniku nr 6 do Instrukcji Zarządzania SI UMK). Podpisanie tego Oświadczenia musi odbyć się przed przyznaniem mu identyfikatora użytkownika.
  18. Co najmniej raz do roku, a w przypadku aplikacji przetwarzających informacje chronione – co sześć miesięcy, Administrator Techniczny jest zobowiązany do przeprowadzenia weryfikacji kont w aplikacji lub oprogramowaniu systemowym, za które jest odpowiedzialny. Administrator Bezpieczeństwa Informatycznego jest zobowiązany do przygotowania odpowiedniej procedury, zgodnie z którą będzie prowadzona ta weryfikacja.
  19. Po wyrejestrowaniu użytkownika z Systemu, jego konta zostają zablokowane,

a następnie po upływie trzech miesięcy – usunięte. Natomiast identyfikator użytkownika nie może zostać usunięty z ewidencji użytkowników nawet po wyrejestrowaniu takiego użytkownika.

### § 3

#### Zasady pracy w SI UMK

1. Przed dopuszczeniem do pracy w SI UMK każda osoba powinna być zaznajomiona z niniejszą Instrukcją.
2. Każdorazowo bezpośredni dostęp do informacji chronionych przetwarzanych w SI UMK jest możliwy jedynie po uwierzytelnieniu i autoryzacji użytkownika (każdego, w tym także Administratora).
3. Okres poza godzinami pracy Urzędu ( godziny pracy Urzędu są traktowane jako od poniedziałku do piątku od godz. 7:30 do godz. 18:00) jest przeznaczony na wykonywanie prac konserwacyjnych w SI UMK. W związku z tym, wprowadza się następujące zasady korzystania z SI UMK poza godzinami pracy Urzędu:
  - a) w przypadku konserwacyjnych wyłączeń całego Systemu lub jego elementów, Administrator Systemu odpowiedzialny za obszar Systemu który podlega wyłączeniu obowiązany jest umieścić na stronie intranetowej UMK komunikat informujący o planowanym wyłączeniu,
  - b) komunikat, o którym mowa w lit. a) powinien zostać umieszczony na stronie intranetowej najpóźniej do godziny 12:00 dnia, w którym planowane jest wyłączenie oraz powinien on zawierać dane kontaktowe do zgłaszania uwag przez użytkowników,
  - c) w przypadku nie zgłoszenia uwag przed użytkownikom Systemu do godz. 15:30 dnia, w którym planowane jest wyłączenie – wyłączenie to zostaje zatwierdzone i nie może zostać odwołane.
4. W przypadkach które zagrażają Bezpieczeństwu Informacji Chronionych przetwarzanych w SI UMK lub samemu SI UMK Administrator Systemu lub Administrator Informacji przetwarzanych w SI może po powiadomieniu Dyrektora Magistratu zawiesić jego pracę bez stosowania się do zasad zawartych w pkt.3.
5. W przypadkach stwierdzenia naruszenia Bezpieczeństwa Informacji Chronionych lub Bezpieczeństwa SI UMK, należy niezwłocznie powiadomić o tym bezpośredniego przełożonego, Administratora Bezpieczeństwa Informatycznego lub osobę przez niego upoważnioną.
6. Osoba użytkująca przenośne urządzenie komputerowe (laptop), obowiązana jest zachować szczególną ostrożność podczas użytkowania, transportu lub przechowywania tego urządzenia poza UMK, a w szczególności powinna:
  - a) zabezpieczyć dostęp do urządzenia w przynajmniej jeden z dostępnych sposobów (np. PIN, hasło itp.),
  - b) zabezpieczyć dostęp do Informacji Chronionych przetwarzanych na tym urządzeniu poprzez zaszyfrowanie tych danych,
  - c) nie zezwalać na używanie tego urządzenia osobom nieuprawnionym.
7. W przypadku utworzenia zbioru danych zawierających dane osobowe, na lokalnym lub przenośnym urządzeniu komputerowym tj. na komputerze typu PC lub laptopie itp. kierownik jednostki organizacyjnej w której jest eksploatowane to urządzenie komputerowe musi wyznaczyć Administratora Danych dla tego zbioru danych. Administratora Danych tego zbioru wskazuje się Administratorowi Informacji przetwarzanych w SI podczas uzyskiwania jego akceptacji.
8. W przypadku awarii SI UMK jego praca zostaje zawieszona na czas usunięcia



- przyczyn awarii. Administrator Techniczny lub Administrator Systemu musi o zaistniałej awarii oraz o przewidywanej przerwie poinformować Administratora Informacji przetwarzanych w SI lub Dyrektora Magistratu.
9. Instalacji oraz aktualizacji Oprogramowania Systemowego i aplikacji dokonuje wyłącznie Administrator Techniczny lub osoby przez niego upoważnione.
  10. Zabrania się użytkownikowi SI UMK:
    - 1) Podejmować prób wykorzystania obcych identyfikatorów użytkownika (kont) i uruchamiania aplikacji deszyfrujących (łamiących) hasła chyba, że użytkownik jest Administratorem Systemu, Administratorem Technicznym lub Administratorem Bezpieczeństwa Informatycznego i prowadzi te działania w celu zapewnienia ochrony informacji (np. testowanie zabezpieczeń) przetwarzanych w SI UMK.
    - 2) Prowadzenia działań mających na celu nieautoryzowany dostęp do Informacji Chronionych przetwarzanych w SI UMK lub podsłuchiwanie czy przechwytywanie informacji przepływających w sieci komputerowej, chyba, że użytkownik jest Administratorem Systemu, Administratorem Technicznym lub Administratorem Bezpieczeństwa Informatycznego i prowadzi te działania w celu zapewnienia ochrony informacji (np. testowanie zabezpieczeń) przetwarzanych w SI UMK.
    - 3) Udostępniać osobom trzecim informacji na temat struktury technicznej SI UMK (w tym adresacji sieci, struktur aplikacji, baz danych itp.) bez zgody Administratora Informacji przetwarzanych w SI, chyba, że użytkownik jest Administratorem Systemu, Administratorem Technicznym lub Administratorem Bezpieczeństwa Informatycznego.
    - 4) Samodzielnej instalacji oprogramowania systemowego i aplikacji chyba, że użytkownik jest Administratorem Systemu lub Administratorem Technicznym.
    - 5) Uruchamianie aplikacji i programów które mogą zakłócić i destabilizować pracę SI UMK, bądź naruszyć bezpieczeństwo danych w nim przetwarzanych.
    - 6) Wysyłania niechcianej przez odbiorcę poczty elektronicznej – tzw. *spamu* oraz wysyłania poczty elektronicznej do losowych odbiorców.

#### **§ 4**

#### **Zabezpieczenia SI UMK**

1. Zdalny dostęp do SI UMK dla pracowników UMK oraz zdalny i lokalny dostęp do SI UMK dla osób nie będących pracownikami UMK określa Regulamin przyznawania zdalnego dostępu do SI UMK, stanowiący załącznik nr 6 do Instrukcji Zarządzania SI UMK.
2. Odpowiedni Administrator Systemu jest zobowiązany przygotować instrukcje wykonywania i odtwarzania kopii awaryjnych informacji chronionych przetwarzanych w SI UMK oraz kopii awaryjnych samego Systemu.
3. Za poprawność powyższych kopii awaryjnych odpowiedzialny jest Administrator Systemu.
4. Kopie awaryjne muszą być przechowywane w kasie pancerniej odpornej na wysokie temperatury, duże pola magnetyczne oraz niszczące działanie czynników zewnętrznych.
5. Czas przechowywania kopii awaryjnych określają instrukcje, o których mowa w pkt.2.
6. Administrator Techniczny zobowiązany jest pozbawić zapisu lub uszkodzić urządzenia komputerowe lub inne nośniki danych, zawierające Informacje Chronione, przeznaczone do likwidacji lub do wykluczenia z SI UMK.

7. Administrator Techniczny zobowiązany jest niezwłocznie odpowiednio oznaczyć identyfikator użytkownika w ewidencji użytkowników, zablokować konto oraz podjąć inne stosowne działania w celu uniemożliwienia dostępu do SI UMK użytkownikowi, który utracił uprawnienia do pracy w SI UMK.
8. Urządzenia komputerowe przetwarzające informacje chronione konserwowane są co najmniej raz na pół roku. W innych przypadkach częstotliwość konserwacji ustala Administrator Systemu lub Administrator Techniczny.
9. Konserwacji urządzeń komputerowych dokonuje osoba wyznaczona przez Administratora Systemu lub Administratora Technicznego.

## **§ 5**

### **Postanowienia końcowe**

1. Administrator Bezpieczeństwa Informatycznego przygotowuje Politykę Bezpieczeństwa SI UMK, w której określi co najmniej:
  - a) szczegółowe zasady dostępu do informacji chronionych, przetwarzanych w SI UMK,
  - b) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są informacje chronione w SI UMK, a w szczególności dane osobowe,
  - c) szczegółowy podział SI UMK na odpowiednie obszary zróżnicowane pod względem bezpieczeństwa: Intranet, Extranet, DMZ itp.,
  - d) wykaz zbiorów danych zawierających informacje chronione, (w szczególności dane osobowe) w SI UMK wraz ze wskazaniem aplikacji zastosowanych do przetwarzania tych danych,
  - e) opis struktury zbiorów danych (w szczególności danych osobowych) wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,
  - f) sposób przepływu danych pomiędzy poszczególnymi aplikacjami w SI UMK lub poza System,
  - g) wymagania dla aplikacji przetwarzających informacje chronione oraz pozostałych aplikacji wchodzących w skład SI UMK,
  - h) opis postępowania w przypadku wystąpienia sytuacji kryzysowych,
  - i) sposób postępowania z wydrukami i nośnikami danych zawierającymi informacje chronione przetwarzane w SI UMK.
2. Odpowiedni Administrator Systemu określa warunki techniczne oraz jest odpowiedzialny za funkcjonowanie i udostępnianie usług dostępnych poprzez sieć komputerową UMK tj. FTP, WWW, poczta elektroniczna. itp.
3. Administrator Systemu lub Administrator Techniczny może odmówić uruchomienia usługi sieciowej w sieci komputerowej w przypadku narażenia bezpieczeństwa informacji chronionych przetwarzanych w SI UMK lub samego Systemu.

## **Regulamin korzystania z urządzeń komputerowych UMK**

### **§ 1**

#### **Przepisy ogólne.**

1. Urządzenie komputerowe, należy użytkować zgodnie z zaleceniami zawartymi w instrukcji obsługi, bądź przekazanymi przez Administratora Technicznego.
2. Stanowisko pracy użytkownika musi być urządzone zgodnie z obowiązującymi przepisami BHP.
3. Monitory urządzeń komputerowych, w pomieszczeniach gdzie dostęp mają osoby nieuprawnione do przetwarzania informacji chronionych muszą być ustawione w sposób uniemożliwiający odczytanie tych informacji przez osoby nieuprawnione.
4. Każdorazowo podczas opuszczania stanowiska pracy gdzie obsługiwane jest urządzenie komputerowe, należy blokować dostęp do tego stanowiska poprzez zablokowanie lub wylogowanie sesji użytkownika.
5. Miejsce, w którym jest zlokalizowane urządzenie komputerowe musi być zabezpieczone przed możliwością jego uszkodzenia przez spadające przedmioty, płyny lub inne czynniki zewnętrzne.
6. W trakcie obsługi urządzenia komputerowego oraz na stanowisku pracy, na którym umieszczone są urządzenia komputerowe nie wolno spożywać posiłków oraz palić papierosów.
7. Urządzenia komputerowe należy utrzymywać w czystości, tzn. dbać o jego estetyczny wygląd zewnętrzny oraz unikać przypadkowego zabrudzenia.
8. Do czyszczenia urządzeń komputerowych należy używać tylko środków do tego przeznaczonych jak pianki, aerozole, ściereczki nasączone lub inne tego rodzaju środki z wyraźnie opisanym przeznaczeniem. W przypadku braku ww. środków czyszczących, dopuszczalne jest używanie miękkich wilgotnych szmatek (nie mokrych), zwilżonych wodą z dodatkiem płynnych detergentów. Zabrania się używania wszelkiego rodzaju rozpuszczalników i zmywaczy powszechnie stosowanych do farb i lakierów takich jak aceton, trójchloroetylen (TRI) benzyna itp. W razie wątpliwości jakich materiałów można użyć do czyszczenia urządzeń komputerowych należy zwrócić się do Administratora Technicznego lub do osoby przez niego upoważnionej.
9. O wszelkich zauważonych mechanicznych uszkodzeniach sieci komputerowej, urządzeń komputerowych oraz instalacji elektrycznej należy poinformować Administratora Technicznego lub osobę przez niego upoważnioną.

### **§ 2**

#### **Korzystanie z urządzeń komputerowych**

1. Wszelkie prace związane z podłączaniem i uruchamianiem urządzeń komputerowych muszą się odbywać przy udziale lub za wiedzą odpowiedniego Administratora Technicznego lub osób przez niego upoważnionych.
2. Zabronione jest:
  - 1) przekazywanie użytkownikowi do eksploatacji niesprawnych lub nieskonfigurowanych urządzeń komputerowych,
  - 2) samodzielne przemieszczanie przez użytkownika urządzeń komputerowych nie będących urządzeniem przenośnym (np. laptop) w inne miejsce bez zgody

- i wiedzy Administratora Technicznego lub osób przez niego upoważnionych.
3. Planowane przemieszczenia urządzeń komputerowych należy uzgodnić z Administratorem Technicznym co najmniej dzień przed terminem ich przemieszczenia.
  4. W przypadku, gdy urządzenie komputerowe podłączone są do sieci elektrycznej poprzez rozdzielacz zasilania tzw. „ACAR”, do tego rozdzielacza bezwzględnie nie wolno podłączać dodatkowych urządzeń elektrycznych, tj. czajników, grzałek, kserokopiarek, odkurzaczy, itp.
  5. Przy korzystaniu z sieci energetycznej dedykowanej wyłącznie dla urządzeń komputerowych posiadającej oznaczone gniazda zasilania, należy zwracać uwagę by do tych gniazd nie podłączać innych urządzeń elektrycznych, w szczególności pobierających dużą moc tj. czajników elektrycznych, termowentylatorów, pieców olejowych itp.
  6. Przy korzystaniu z sieci elektrycznej z awaryjnym podtrzymaniem zasilania wolno przyłączać do niej wyłącznie urządzenia wyznaczone przez Administratora Technicznego lub osoby przez niego upoważnione.
  7. Materiały eksploatacyjne używane w urządzeniach komputerowych tj. nośniki danych, materiały eksploatacyjne do drukarek itp. powinny odpowiadać normom określonym przez producenta urządzeń komputerowych.
  8. Nie wolno stosować materiałów eksploatacyjnych nieoznaczonych oraz niewiadomego pochodzenia.

### **§ 3** **Inwentarz**

1. Osoba eksploatująca urządzenie komputerowe ponosi za nie pełną odpowiedzialność, w rozumieniu przepisów kodeksu cywilnego oraz kodeksu pracy.
2. W momencie wydania urządzeń komputerowych do eksploatacji
  - 1) zakładana jest Karta użytkownika zawierająca:
    - imię i nazwisko osoby odpowiedzialnej za urządzenie komputerowe,
    - datę przyjęcia urządzenia komputerowego do eksploatacji oraz datę jego przekazania innej osobie,
    - identyfikator urządzenia komputerowego nadany przez Administratora Technicznego,
    - nazwę Oprogramowania Systemowego zainstalowanego na urządzeniu komputerowym,
    - identyfikatory dodatkowych urządzeń komputerowych stanowiących wraz z podstawowym urządzeniem komputerowym zestaw zdolny do eksploatacji,
  - 2) w widocznym miejscu naklejany jest jego identyfikator.
3. Identyfikator urządzenia komputerowego określa jego nazwę w Systemie Informatycznym oraz w ewidencji urządzeń komputerowych. Ewidencja urządzeń komputerowych zawiera pełne i kompletne informacje o danym urządzeniu komputerowym.
4. Ewidencję urządzeń komputerowych prowadzi odpowiedni Administrator Systemu. Ewidencja ta ma charakter informacji chronionych. Każda osoba eksploatująca urządzenie komputerowe ma prawo wglądu w ewidencję w zakresie danych dotyczących tego urządzenia komputerowego.
5. Pierwszego wpisu do karty użytkownika dokonuje Administrator Techniczny lub osoba przez niego uprawniona, zaś następne wpisy dokonuje bezpośredni przełożony

- osoby odpowiedzialnej za sprzęt komputerowy, każdorazowo powiadamiając o tym fakcie Administratora Technicznego lub osobę przez niego upoważnioną.
6. Oryginały Kart użytkownika przechowuje odpowiedni Administrator Systemu lub osoby przez niego upoważnione.
  7. Osoba eksploatująca urządzenie komputerowe zobowiązana jest dbać o jego kompletność oraz prawidłowość eksploatacji.
  8. W przypadku niemożności ustalenia osoby odpowiedzialnej za urządzenie komputerowe odpowiada za nie osoba kierująca tą jednostką organizacyjną, w której eksploatowane jest urządzenie komputerowe.
  9. Osoba, która w związku z ustaniem stosunku pracy wypełnia kartę obiegową musi uzyskać:
    - 1) potwierdzenie odpowiedniego oznaczenia jej identyfikatora użytkownika i zablokowania kont dostępu do SI UMK od Administratora Systemu,
    - 2) wpis do Karty użytkownika potwierdzony przez przełożonego o zakończeniu eksploatacji urządzenia komputerowego.

#### **§ 4** **Serwis**

1. Wszelkie awarie i nieprawidłowości w pracy urządzeń komputerowych należy zgłaszać Administratorowi Technicznemu lub osobom przez niego upoważnionym.
2. Serwis urządzeń komputerowych prowadzi wyłącznie odpowiedni Administrator Systemu, Administrator Techniczny lub osoba przez niego upoważniona.
3. Na czas serwisu urządzenia komputerowego odpowiedzialność za nie ponosi Administrator Techniczny lub Administrator Systemu bez konieczności wpisu w Kartę użytkownika.
4. Niedopuszczalny jest samodzielny serwis urządzenia komputerowego lub jego rozmontowywanie.
5. Przy przekazywaniu urządzenia komputerowego do serwisu należy zadbać o otrzymanie od Administratora Technicznego pisemnego potwierdzenia przejęcia go do serwisu.
6. W przypadku awarii lokalnego urządzenia komputerowego, na którym założony został lokalny Zbiór danych zawierający Informacje Chronione Administrator Techniczny winien zadbać o Bezpieczeństwo tych Informacji Chronionych, szczególnie przy przekazywaniu tych urządzeń do serwisów specjalistycznych. W tym celu Administrator Techniczny zobowiązany jest pozbawić zapisu przed serwisem urządzenia komputerowego, dysków lub innych nośników danych zawierających Informacje Chronione, albo naprawia się je pod nadzorem Administratora Technicznego.
7. Przy odebraniu urządzenia komputerowego po serwisie użytkownik zobowiązany jest wydać Administratorowi Technicznemu potwierdzenie przejęcia na serwis określone w pkt. 5.

### **Regulamin zakupu, modernizacji, wdrażania i eksploatacji aplikacji**

1. Odpowiedni Administrator Systemu przygotowuje procedurę odbioru, wdrożenia oraz przekazania aplikacji do eksploatacji w SI UMK.
2. Każda jednostka organizacyjna UMK zawierająca umowę, której przedmiot obejmuje wykonanie lub nabycie aplikacji lub projektu aplikacji, musi uzyskać akceptację umowy przez Administratora Informacji przetwarzanych w SI.
3. Umowa, o której mowa w pkt. 2 musi zawierać następujące elementy:
  - a) wskazanie strony umowy będącej właścicielem praw autorskich do aplikacji lub projektu aplikacji,
  - b) dokładne określenie ilości licencji, stanowisk, ról i praw dostępu do aplikacji,
  - c) określenie zasad wdrożenia i szkoleń,
  - d) w przypadku takiej konieczności zgodę Wykonawcy na korzystanie ze struktur, tablic oraz innych obiektów bazy danych wykorzystywanych przez program w celu zabezpieczenia jego praw autorskich,
  - e) określenie warunków gwarancji aplikacji,
  - f) określenie zasad asysty technicznej i konserwacji aplikacji,
  - g) zabezpieczenie kompletnej dokumentacji do aplikacji.
4. Oprócz umowy, o której mowa w pkt. 2 należy sporządzić i przedłożyć kosztorys zawierający łączne koszty wdrożenia i eksploatacji aplikacji, który obejmuje:
  - a) koszt nabycia wdrażanej aplikacji,
  - b) całkowity koszt wdrożenia aplikacji (szkolenia, asysta techniczna przy wdrożeniu itp.)
  - c) koszt dodatkowych urządzeń komputerowych oraz innych aplikacji i oprogramowania systemowego, które są niezbędne do prawidłowej eksploatacji wdrażanej aplikacji,
  - d) koszt asysty technicznej i konserwacji na wdrażaną aplikację.
5. Podpisanie umowy wskazanej w pkt. 2 musi być poprzedzone uzgodnieniami z Administratorem Systemu w formie protokołu uzgodnień następujących tematów:
  - a) miejsca zlokalizowania, ilości oraz parametrów technicznych urządzeń komputerowych, na których będzie zainstalowana i używana aplikacja.
  - b) zasad i osób odpowiedzialnych za administrację aplikacji oraz jej wpływ na obciążenie i pracę SI UMK,
  - c) wskazania Merytorycznego Administratora Informacji przetwarzanych w tej aplikacji oraz Gospodarza aplikacji.

## **Regulamin udostępniania danych oraz rejestracji zbiorów danych osobowych**

### **§ 1**

#### **Udostępnianie danych przetwarzanych w SI UMK**

1. Za udostępnianie informacji chronionych poza SI UMK odpowiada Administrator Informacji przetwarzanych w SI lub odpowiedni Merytoryczny Administrator Informacji.
2. Za udostępnienie pozostałych informacji przetwarzanych w SI UMK, odpowiada użytkownik merytorycznie odpowiedzialny za udostępnianie tych danych.
3. Udostępnienie danych osobowych w formie elektronicznej, poprzez urządzenia teletransmisji poza SI UMK możliwe jest jedynie po zastosowaniu metod kryptograficznych (połączenie szyfrowane lub szyfracja danych).
4. Udostępnienie zbiorów danych zawierających informacje chronione może nastąpić wyłącznie po wyrażeniu zgody przez Administratora Informacji przetwarzanych w SI lub odpowiedniego Merytorycznego Administratora Informacji.
5. W przypadku udostępniania danych w postaci elektronicznej, format i sposób udostępnienia tych danych określa Administrator Systemu lub Administrator Techniczny. W przypadku udostępniania danych w postaci elektronicznej, Administrator Systemu może odmówić udostępnienia tych danych w takiej formie, jeżeli może to naruszyć bezpieczeństwo i ochronę pozostałych informacji przetwarzanych w SI UMK lub samego SI UMK.

### **§ 2**

#### **Rejestracja zbiorów danych osobowych**

1. Zbiory danych zawierające dane osobowe przetwarzane w SI UMK, w tym także zbiory danych zawierające dane osobowe umieszczone na lokalnych lub przenośnych urządzeniach komputerowych (np. komputery typu PC lub laptopy) rejestruje Administrator Informacji przetwarzanych w SI zgodnie z Ustawą o ochronie danych osobowych.
2. W przypadku nie uzyskania akceptacji Administratora Informacji przetwarzanych w SI dla przetwarzania danych osobowych w lokalnym zbiorze danych na lokalnym lub przenośnym urządzeniu komputerowym, Administratorem danych w rozumieniu Ustawy o ochronie danych osobowych dla tego lokalnego zbioru danych jest użytkownik obsługujący dane urządzenie komputerowe. W szczególności użytkownik ten odpowiada za rejestrację tego zbioru danych zgodnie z Ustawą o ochronie danych osobowych oraz za Bezpieczeństwo danych osobowych w nim przetwarzanych.

## **Regulamin przyznawania dostępu do SI UMK**

### **§ 1 Pracownicy UMK.**

1. Dostęp do SI UMK może uzyskać każdy pracownik UMK, który wypełni odpowiedni wniosek, którego wzór stanowi załącznik nr 1 do niniejszego regulaminu oraz prześle go do Administratora Informacji przetwarzanych w SI.
2. Zdalny dostęp do SI UMK, może uzyskać każdy pracownik UMK, który:
  - a) wypełni odpowiedni wniosek, którego wzór stanowi załącznik nr 2 do niniejszego regulaminu oraz prześle go do Administratora Informacji przetwarzanych w SI
  - b) wykaże w powyższym wniosku, iż taki dostęp jest mu niezbędny do realizacji powierzonych zadań służbowych.
3. Dostęp do aplikacji SI UMK, lub zmianę uprawnień w aplikacjach SI UMK, uzyskuje każdy pracownik UMK, który wypełni odpowiedni wniosek, którego wzór stanowi załącznik nr 3 do niniejszego regulaminu oraz prześle go do Administratora Informacji przetwarzanych w SI.
4. Wypełniony wniosek akceptuje Administrator Informacji przetwarzanych w SI i przekazuje go do realizacji do odpowiedniego Administratora Systemu.
5. Każda komórka organizacyjna UMK może przedłożyć jeden wspólny wniosek dla kilku swoich pracowników.
6. Osobą upoważnioną do przedłożenia wniosku, jest Merytoryczny Administrator Informacji.
7. Przed otrzymaniem dostępu do SI UMK oraz przed otrzymaniem identyfikatora użytkownika, każdy pracownik UMK musi podpisać oświadczenie o zachowaniu poufności, stanowiące zał. nr 7 Instrukcji.
8. Oryginały wniosków i podpisanych oświadczeń przechowywane są u Administratora Bezpieczeństwa Informacji.

### **§ 2 Osoby nie będące pracownikami UMK.**

1. Dostęp do SI UMK mogą posiadać także osoby zewnętrzne:
  - a) pracownicy miejskich jednostek organizacyjnych,
  - b) pracownicy podmiotów nie ujętych powyżej na podstawie odrębnej umowy (np. umowy o świadczenie usługi wsparcia technicznego)
  - c) inne osoby zewnętrzne.
2. Osoby zewnętrzne, o których mowa w pkt. 1 ubiegające się o dostęp do SI UMK muszą przedłożyć odpowiedni wniosek, którego wzór przedstawiono w załączniku nr 1 do niniejszego regulaminu.
3. Każda miejska jednostka organizacyjna oraz każdy podmiot może przedłożyć jeden wspólny wniosek dla kilku swoich pracowników.
4. Osobą upoważnioną do przedłożenia wniosku, jest kierujący miejską jednostką organizacyjną lub podmiotem.
5. Wypełniony wniosek akceptuje Administrator Informacji przetwarzanych w SI i przekazuje go do realizacji do odpowiedniego Administratora Systemu.



6. Przed otrzymaniem dostępu do SI UMK oraz przed otrzymaniem identyfikatora użytkownika, każda osoba zewnętrzna musi podpisać oświadczenie o zachowaniu poufności, stanowiące zał. nr 7 Instrukcji...
7. Oryginały wniosków i podpisanych oświadczeń przechowywane są u Administratora Bezpieczeństwa Informacji.

## FORMULARZ ZGŁOSZENIOWY

### Wniosek o przyznanie dostępu do Systemu Informatycznego UMK dla pracowników UMK.

<b>Data wypełnienia formularza:</b>	
-------------------------------------	--

**Proszę o przyznanie, dla wymienionych poniżej osób:**

- dostępu do SI UMK<sup>1</sup>,
- identyfikatora użytkownika<sup>1</sup>,
- konta pocztowego e-mail<sup>1</sup>.

**Dane osób zgłaszanych:**

Lp.	Imię i Nazwisko:	Nr telefonu:	Symbol komórki org. UMK:	Okres obowiązywania uprawnień <sup>2</sup>
1.				
2.				
3.				
4.				
5.				
6.				

---

<sup>1</sup> Niepotrzebne skreślić.

<sup>2</sup> **Należy wpisać „bezterminowy” lub odpowiednią datę.** Dostęp do SI UMK może zostać przyznany na okres bezterminowy lub na okres czasowy.

Kraków, dnia .....

.....  
Imię i nazwisko osoby wypełniającej wniosek.

.....  
Komórka organizacyjna UMK/ Miejska Jednostka Organizacyjna  
/Nazwa firmy\*

**W N I O S E K**  
**O PRYZNANIE DOSTĘPU DO SI UMK**

Proszę o przyznanie dostępu do Systemu Informatycznego Urzędu Miasta Krakowa oraz przyznanie Identyfikatorów Użytkownika w SI UMK\*, w celu:

.....  
dla następujących osób:

LP.	Imię i Nazwisko
1.	
2.	
3.	

Dostęp ma być przyznany:\*

- a) na czas nieokreślony,
- b) na okres od..... do .....

Dostęp ma być przyznany:\*

- a) bezpośrednio
- b) zdalnie

Lista zadań przewidzianych do realizacji w SI UMK z wykorzystaniem tego dostępu:

- 1.
- 2.
- 3.

Jednocześnie zobowiązuję się do pokrycia kosztów związanych z usuwaniem ewentualnych uszkodzeń SI UMK, jakie mogą być następstwem działań osób uzyskujących dostęp. Roszczeń odszkodowawczych wynikających z powstałej szkody, Urząd Miasta Krakowa dochodzić będzie na zasadach ogólnych, w postępowaniu przed sądem właściwym dla siedziby Urzędu.

.....  
Akceptacja Administratora Informacji  
przetwarzanych w SI

.....  
Podpis osoby wypełniającej wniosek

-----  
\*niepotrzebne skreślić

## FORMULARZ ZGŁOSZENIOWY

### Wniosek o przyznanie lub zmianę uprawnień do aplikacji SI UMK dla pracowników UMK.

<b>Data wypełnienia formularza:</b>	
<b>Nazwa aplikacji:</b>	

#### Dane osób zgłaszanych:

Lp.	Imię i Nazwisko:	Nr telefonu:	Symbol komórki org. UMK:	Nazwa identyfikatora użytkownika w SI UMK <sup>1</sup> :	Przyznanie / zmiana uprawnień <sup>2</sup> :
1.					
2.					
3.					
4.					

#### Poziom uprawnień użytkownika w aplikacji lub inne uwagi<sup>3</sup>:

Lp.	Nazwa identyfikatora użytkownika w SI UMK:	Uwagi:
1.		
2.		
3.		
4.		

<sup>1</sup> Należy wpisać nazwę użytkownika w SI UMK, jeśli brak – należy pozostawić rubrykę pustą i równocześnie złożyć osobny formularz o przyznanie dostępu do SI UMK.

<sup>2</sup> Należy wpisać **przyznanie** lub **zmiana**, w zależności od tego czy wnioskuję się o nowe uprawnienia, czy też o zmianę istniejących uprawnień.

<sup>3</sup> Należy wpisać żądany poziom uprawnień (jeśli aplikacja ma taką funkcjonalność lub jeśli dotyczy) albo inne uwagi (np. przejęcie zadań i uprawnień innej osoby itp.).

Kraków, dnia .....

.....  
Imię i Nazwisko

.....  
Komórka organizacyjna UMK/ Miejska Jednostka Organizacyjna  
/Nazwa podmiotu

### OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI

W związku z otrzymaniem dostępu do SI UMK, w którym przetwarzane są dane osobowe i do którego mają dostęp tylko autoryzowani użytkownicy, oświadczam, iż zobowiązuję się do:

- a) zachowania w tajemnicy posiadanych haseł i kont w SI UMK,
- b) zmiany haseł do posiadanych kont co najmniej raz na miesiąc,
- c) wykorzystywania posiadanych oraz udostępnionych kont Użytkownika wyłącznie do zadań określonych we wniosku o przyznanie dostępu do SI UMK,
- d) nie podejmowania prób wykorzystania obcych kont i uruchamiania aplikacji deszyfrujących (łamiących) hasła,
- e) nie instalowania samodzielnie, bez zgody administratorów SI UMK oprogramowania systemowego, podsystemów i aplikacji (programów),
- f) nie uruchamiania aplikacji (programów), które mogą zakłócić i destabilizować pracę SI UMK, bądź naruszyć prywatność danych w nim zgromadzonych,
- g) nie udostępniania osobom trzecim informacji na temat struktury informatycznej SI UMK (w tym adresacji sieci, struktur aplikacji, baz danych itp.),
- h) nie pozyskiwania we własnym zakresie (bez odpowiednich, wcześniejszych ustaleń) jakichkolwiek danych z SI UMK. W szczególności dotyczy to danych osobowych, które mogą być przekazane poza SI UMK jedynie za zgodą Administratora Danych UMK i każdorazowo po podpisaniu pisemnego protokołu przekazania danych osobowych,
- i) niezwłocznego poinformowania administratorów SI UMK o wykryciu nieautoryzowanego dostępu do danych przetwarzanych w SI UMK.

Jednocześnie przyjmuję do wiadomości, iż moje działania w SI UMK mogą być na bieżąco monitorowane oraz będą w pełni lub częściowo logowane.

.....  
czytelny podpis