

Zasady zarządzania bezpieczeństwem informacji w Urzędzie Miasta Krakowa

(Skrócona wersja „Zasad zarządzania bezpieczeństwem informacji w Urzędzie Miasta Krakowa”)

Dokument: wersja 5

Data: 08.11.2018 r.

Zatwierdził: Renata Woyciechowska – Inspektor Ochrony Danych UMK

SPIS TREŚCI

1. Wstęp	3
1.1 Cel dokumentu.....	3
1.2 Zakres i przedmiot stosowania	3
1.3 Definicje.....	3
1.4 Skróty	6
1.5 Zakres i granice PBI.....	6
1.6 Integralna część dokumentacji:	6
2. Bezpieczeństwo prawno–organizacyjne.....	7
2.1 Struktura ról i odpowiedzialności	7
2.1.1 Administrator Danych	7
2.1.2 Inspektor Ochrony Danych	7
2.1.3 Administrator Systemu.....	8
2.1.4 Merytoryczny Administrator Informacji.....	9
2.1.5 Koordynator Polityki Bezpieczeństwa Informacji	9
2.1.6 Administrator Techniczny	10
2.1.7 Gospodarz	10
2.1.8 Pozostałe odpowiedzialności.....	11
2.2 Zarządzanie zbiorami danych.....	11
2.2.1 Udostępnianie informacji chronionych	11
2.2.2 Udostępnianie danych osobowych.....	11
2.2.3 Realizacja praw osoby, której dane dotyczą	12
2.2.4 Zarządzanie upoważnieniami do przetwarzania danych osobowych	12
2.3 Bezpieczeństwo w kontaktach ze stronami trzecimi.....	12
3. Bezpieczeństwo teleinformatyczne	13
3.1 Instrukcja zarządzaniem SI UMK	13
3.2 Zarządzanie upoważnieniami i uprawnieniami	13
3.2.1 Uprawnienia do pracy w SI UMK dla stron trzecich:.....	13
3.2.2 Uprawnienia do pracy zdalnej w SI UMK:	14
5.1.1 Konto użytkownika w SI UMK.....	15
5.1.2 Odpowiedzialność użytkownika.....	15
5.1.3 Ochrona haseł.....	16
4. Formularze:	16
F-11 Wzór wniosku o przyznanie dostępu do SI UMK.....	20
F-29 Oświadczenie o zachowaniu poufności dla stron trzecich	24

1. Wstęp

1.1 Cel dokumentu

Niniejszy dokument określa spójne mechanizmy zarządzania bezpieczeństwem informacji oraz zasady postępowania w celu zapewnienia poufności, dostępności oraz integralności informacji przetwarzanych w Urzędzie Miasta Krakowa.

Celem niniejszego dokumentu jest optymalizacja funkcjonowania Urzędu Miasta Krakowa, obniżenie ryzyka naruszenia bezpieczeństwa informacji, określenie sposobu dostępu do informacji oraz zapewnienie ciągłości działania Urzędu Miasta Krakowa.

1.2 Zakres i przedmiot stosowania

Obowiązek stosowania zasad opisanych w niniejszym dokumencie obejmuje wszystkie komórki organizacyjne Urzędu Miasta Krakowa oraz strony trzecie świadczące usługi na rzecz Urzędu Miasta Krakowa.

1.3 Definicje

Administrator Danych – Prezydent Miasta Krakowa jako organ samorządu terytorialnego decydujący o celach i sposobach przetwarzania danych osobowych oraz informacji chronionych w Urzędzie Miasta Krakowa.

Administrator Systemu – kierujący komórką organizacyjną właściwą dla obszaru informatyki; osoba odpowiedzialna za ciągłość pracy, rozwój oraz bezpieczeństwo Systemów Informatycznych Urzędu Miasta Krakowa.

Administrator Techniczny – osoba odpowiedzialna za techniczny nadzór nad pracą aplikacji, oprogramowania systemowego, sieci komputerowej lub urządzeń komputerowych.

Aktywa – wszystko, co ma wartość dla Urzędu Miasta Krakowa.

Aplikacja – program komputerowy, będący częścią systemu informatycznego oraz przetwarzający informacje.

Autoryzacja – weryfikowanie, czy dany użytkownik ma prawo dostępu do informacji, do których usiłuje uzyskać dostęp.

Błąd – nieprawidłowe działanie aplikacji, oprogramowania systemowego, urządzeń komputerowych, sieci komputerowej lub innych elementów systemu informatycznego, niezgodne z instrukcją użytkownika lub dokumentacją techniczną.

Ciągłość działania – operacyjna i strategiczna zdolność organizacji do reakcji na incydent oraz zakłócenia działania, tak by móc kontynuować działania na możliwym do przyjęcia wcześniej określonym poziomie.

Dane osobowe – dane w rozumieniu art. 4 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), zwanego dalej „RODO”.

Dostępność informacji – właściwość zapewniająca, że informacja przetwarzana w Urzędzie Miasta Krakowa jest dostępna dla osób upoważnionych zawsze wtedy, gdy jest to potrzebne.

Gospodarz – osoba odpowiedzialna za działanie aplikacji pod względem merytorycznym.

Grupa informacji – nieformalny zbiór informacji podobnych pod kątem zawartości informacyjnej i jej wartości dla organizacji.

Hasło – ciąg znaków literowych, cyfrowych lub innych wykorzystywany w procesie uwierzytelniania użytkownika przy uzyskiwaniu dostępu do systemu informatycznego i znany jedynie użytkownikowi.

Identyfikator użytkownika – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę, która jest użytkownikiem systemu informatycznego.

Incydent bezpieczeństwa – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań i zagrażają bezpieczeństwu informacji.

Informacje (dane) – wszystko, co posiada logiczne znaczenie jako przekaz treści i nadaje się do praktycznego wykorzystania w procesach, skutkując osiągnięciem celu. Informacja może być przetwarzana na różnych typach nośników (m.in. papierowych, magnetycznych, optycznych itp.), w szczególności w systemach informatycznych.

Informacje chronione – informacje przetwarzane w Urzędzie Miasta Krakowa, którym Urząd zapewnia bezpieczeństwo i dla których wartość graniczna bezpieczeństwa (WG) została ustalona na poziomie mniejszym lub równym 8 na podstawie analizy ryzyka.

Informacje szczególnie chronione – informacje przetwarzane w Urzędzie Miasta Krakowa, którym Urząd zapewnia bezpieczeństwo i dla których wartość graniczna bezpieczeństwa (WG) została ustalona na poziomie równym 9 na podstawie analizy ryzyka.

Integralność informacji – właściwość zapewniająca, że informacja przetwarzana w Urzędzie Miasta Krakowa nie została zmieniona lub zniszczona w sposób nieautoryzowany, czyli, że została zachowana dokładność i kompletność informacji.

Inspektor Ochrony Danych – osoba, o której mowa w art. 37–39 RODO.

Klasyfikacja informacji – procedura dokonująca klasyfikacji występujących w Urzędzie Miasta Krakowa informacji, odzwierciedlająca potrzeby, priorytety oraz oczekiwany poziom ochrony przy ich przetwarzaniu.

Koordynator Polityki Bezpieczeństwa Informacji – osoba realizująca postanowienia Merytorycznego Administratora Informacji w zakresie Polityki Bezpieczeństwa Informacji.

Kopia zapasowa – duplikat danych, przechowywany na wymiennym nośniku komputerowym, służący do odtworzenia oprogramowania systemowego, aplikacji lub dokumentu.

Merytoryczny Administrator Informacji – kierujący komórką organizacyjną właściwą dla danego zakresu danych, osoba odpowiedzialna merytorycznie za przetwarzanie informacji oraz w dyspozycji, której znajdują się te informacje.

Obszar funkcjonowania – wyodrębniony obszar związany z realizacją procesów.

Operator obsługi incydentu – osoba wyznaczona przez Inspektora Ochrony Danych, której rolą jest podejmowanie działań związanych z usunięciem incydentu.

Oprogramowanie systemowe – systemy operacyjne, bazodanowe lub inne programy, niezbędne do uruchomienia oraz eksploatacji aplikacji.

Plan ciągłości działania – udokumentowany zbiór procedur i informacji, które są opracowane, gromadzone i utrzymywane w stanie gotowym do użycia w przypadku wystąpienia incydentu, by umożliwić organizacji kontynuowanie wykonywanych działań

krytycznych na możliwym do przyjęcia wcześniej określonym poziomie.

Poufność informacji – właściwość zapewniająca, że informacja przetwarzana w Urzędzie Miasta Krakowa jest udostępniana tylko osobom upoważnionym.

Poziom ochrony – określa wrażliwość informacji zgodnie z przyjętą klasyfikacją informacji i wpływa na sposób przetwarzania.

Procedura – opis czynności niezbędnych do zrealizowania wyznaczonego celu.

Procedura awaryjno-odtworzeniowa – procedura zawierająca opis czynności w przypadku wystąpienia określonego zdarzenia wpływającego na ciągłość działania organizacji.

Przetwarzanie informacji – przetwarzanie w rozumieniu art. 4 pkt 2 RODO.

Punkt krytyczny – zagrożenie lub podatność mająca wpływ na przetwarzane informacje, przebieg realizowanego obszaru funkcjonowania lub spełnienie wymagań prawnych dotyczących organizacji. Punkt Krytyczny jest scharakteryzowany następującymi atrybutami:

- częstotliwość wystąpienia punktu krytycznego,
- wpływ na spełnienie wymagań prawnych oraz funkcjonowanie procesu,
- konsekwencje finansowe dla organizacji.

Sieć komputerowa – okablowanie, urządzenia komputerowe oraz oprogramowanie służące do teletransmisji informacji.

System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procesów przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

System Informatyczny Urzędu Miasta Krakowa – system informatyczny służący do przetwarzania informacji Urzędu Miasta Krakowa.

Strony trzecie – podmioty zewnętrzne świadczący usługi dla Urzędu Miasta Krakowa.

Środek przetwarzania informacji – urządzenia służące do przetwarzania informacji, np. drukarka, kserokopiarka, komputer, CD, niszczarka.

Urządzenie komputerowe – urządzenie służące do przetwarzania oraz teletransmisji informacji, np. komputer PC, laptop, serwer, urządzenie sieciowe, palmtop.

Urządzenie peryferyjne – dodatkowe, opcjonalne wyposażenie urządzenia komputerowego np. skaner, pendrive, kamera internetowa.

Uwierzytelnianie – jednoznaczna identyfikacja użytkownika lub urządzenia.

Użytkownik – uprawniona osoba, która uzyskała dostęp i korzysta z zasobów Systemu Informatycznego Urzędu Miasta Krakowa.

Zabezpieczenie – rozwiązanie techniczne lub organizacyjne minimalizujące ryzyko.

Zbiór danych – zbiór w rozumieniu art. 4 pkt 6 RODO, mogący zawierać dane osobowe.

Zbiór danych osobowych – zbiór danych w rozumieniu art. 4 pkt 6 RODO.

1.4 Skróty

IOD – Inspektor Ochrony Danych

AD – Administrator Danych

AS – Administrator Systemu

AT – Administrator Techniczny

MAI – Merytoryczny Administrator Informacji

PBI – Polityka Bezpieczeństwa Informacji

PCD – Plan Ciągłości Działania

PMK – Prezydent Miasta Krakowa

RODO – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1)

SI – System Informatyczny

SI UMK – System Informatyczny Urzędu Miasta Krakowa

SZBI – System Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Krakowa

SZJ – System Zarządzania Jakością w Urzędzie Miasta Krakowa

UMK – Urząd Miasta Krakowa

ZCD – Zarządzanie Ciągłością Działania

1.5 Zakres i granice PBI

Rodzaj działalności: administracja samorządowa szczebla gminy i powiatu

Informacje o wyrobie: akt prawa miejscowego, uchwała, zarządzenie, polecenie, upoważnienie, pełnomocnictwo, dotacja, decyzja administracyjna, zaświadczenie, postanowienie, opinia, informacja.

Fizyczne umiejscowienie działalności: 34 lokalizacje na terenie Miasta Krakowa z siedzibą główną na Placu Wszystkich Świętych 3-4

Najistotniejsze aktywa: personel, informacje, SI UMK, infrastruktura

Granice logiczne organizacji: UMK prowadzi działalność na terenie Gminy Miejskiej Kraków.

Wyłączenia dotyczące zakresu oraz wymagań normy ISO 27001: brak

1.6 Integralna część dokumentacji:

Integralną część dokumentacji Zasad zarządzania bezpieczeństwem informacji w Urzędzie Miasta Krakowa stanowią załączniki:

- Załącznik nr 1 – Dokumenty PBI (procedury, instrukcje, regulaminy, wykazy, itd)
- Załącznik nr 2 – Formularze PBI (wzory dokumentów)

O udostępnianiu tych dokumentów decyduje IOD.

2. Bezpieczeństwo prawno-organizacyjne

Bezpieczeństwo prawno-organizacyjne to zabezpieczenie interesów UMK poprzez zbudowanie skutecznych rozwiązań organizacyjnych, uświadomienie pracownikom konieczności przestrzegania określonych reguł wynikających z obowiązujących przepisów, nadzorowanie i dostosowanie działań UMK do obowiązujących przepisów prawnych. Ze względu na to rozdział uszczegóławia:

- Strukturę ról i odpowiedzialności,
- Proces zarządzania bezpieczeństwem informacji,
- Inwentaryzację/ewidencję aktywów,
- Zarządzanie zbiorami informacji chronionych,
- Zasady ochrony danych osobowych,
- Klasyfikację i oznaczanie informacji oraz postępowanie z informacjami należącymi do określonego poziomu ochrony,
- Bezpieczeństwo w kontaktach ze stronami trzecimi.

2.1 Struktura ról i odpowiedzialności

Odnosi się do wymagania systemu zarządzania bezpieczeństwem informacji określenia odpowiednich ról oraz przypisania im odpowiedzialności w zakresie bezpieczeństwa informacji. Role w zakresie koordynacji bezpieczeństwa informacji w UMK pełnią: AD, IOD, AS, MAI, Koordynator PBI, Gospodarz, AT.

2.1.1 Administrator Danych

- Ustala cele i sposoby przetwarzania danych osobowych
- Wprowadza i zatwierdza SZBI.
- Zapewnia niezbędne zasoby potrzebne do odpowiedniego funkcjonowania bezpieczeństwa informacji w UMK.
- Wydaje upoważnienia do przetwarzania danych osobowych na wniosek kierujących komórkami organizacyjnymi UMK.
- Prowadzi rejestr użytkowników upoważnionych do przetwarzania danych osobowych.
- Wyznacza IOD.
- Zapewnia środki i organizacyjną odrębność IOD niezbędną do wykonywania zadań określonych w art. 39 RODO.
- Zatwierdza kierunki rozwoju i doskonalenia SZBI.

2.1.2 Inspektor Ochrony Danych

- Realizuje zadania określone w art. 39 RODO
- Jest odpowiedzialny przed AD za zapewnienie przestrzegania przepisów o ochronie danych osobowych.
- Nadzoruje opracowanie i aktualizację dokumentów SZBI.
- Dokonuje sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych

- Sporządza dla AD sprawozdanie z przestrzegania zasad bezpieczeństwa informacji.
- Prowadzi rejestr czynności przetwarzania danych przetwarzanych przez AD.
- Odpowiada za przeprowadzenie klasyfikacji informacji w UMK.
- Odpowiada za przeprowadzenie analizy ryzyka w zakresie bezpieczeństwa informacji.
- Nadzoruje i monitoruje przestrzeganie zasad ochrony przetwarzanych informacji w UMK.
- Opracowuje system szkoleń z zakresu bezpieczeństwa informacji oraz nadzoruje ich przeprowadzanie.
- Zarządza incydentami bezpieczeństwa informacji.
- Prowadzi rejestr incydentów bezpieczeństwa, analizuje incydenty oraz wszczyna postępowanie wyjaśniające w związku z incydentami.
- Zarządza kartami elektronicznymi wydawanymi w UMK.
- Jest odpowiedzialny przed PMK za prawidłowe funkcjonowanie SZBI w zakresie normy ISO 27001.
- Jest odpowiedzialny za zgodność zasad i reguł opisanych w ramach SZBI zgodnie z wymaganiami normy ISO 27001.
- Przygotowuje dane wejściowe na przegląd zarządzania SZJ organizowany przez kierownictwo UMK.
- Ustala terminy oraz organizuje przeglądy SZBI
- Odpowiada za doskonalenie i rozwój SZBI
- Podejmuje działania zapobiegawcze i korygujące w ramach SZBI.
- Koordynuje zarządzanie ciągłością działania oraz utrzymuje wykaz PCD.
- Odpowiada za deklarację stosowania oraz pomiar skuteczności zabezpieczeń.

2.1.3 Administrator Systemu

- Zarządza SI UMK.
- Wyznacza AT, w tym zakres zadań w ramach obowiązków AT oraz nadzoruje ich pracę.
- Nadzoruje stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych w SI UMK informacji, a w szczególności odpowiada za zabezpieczenie tych danych przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem.
- Nadzoruje administrowanie SI UMK.
- Nadzoruje prowadzenie bieżącej ewidencji wszystkich użytkowników SI UMK.
- Nadzoruje działania zapewniające sprawne funkcjonowanie i zabezpieczenie SI UMK przed niepowołanym dostępem.
- Ewidencjonuje aplikacje oraz urządzenia komputerowe, które są niezbędne do realizacji zadań komórek organizacyjnych UMK.
- Opiniuje wdrażanie aplikacji i zakup urządzeń komputerowych przez komórki organizacyjne UMK.
- Nadzoruje rozbudowę SI UMK oraz wprowadzanie nowych technologii.

- Nadzoruje wdrażanie aplikacji w SI UMK oraz zapewnienie ciągłości ich pracy ze strony technicznej.
- Administruje licencjami SI UMK.
- Odpowiada za doskonalenie i unowocześnianie SI UMK
- Współpracuje z IOD w zakresie SZBI

2.1.4 Merytoryczny Administrator Informacji

- Odpowiada za identyfikowanie zbiorów danych, ich opisanie i zgłoszenie IOD.
- Odpowiada za zarządzanie wyznaczonym zbiorem danych.
- Odpowiada za poprawność merytoryczną danych zawartych w zbiorze oraz ich aktualizację.
- Odpowiada za aktualizację informacji o zbiorze danych i poinformowanie IOD o zmianach dotyczących zbioru.
- Określa narzędzia, metody, miejsce i czas przetwarzania informacji w zbiorze danych.
- Wyraża zgodę wnioskującym na przetwarzanie informacji w powierzonym zbiorze danych.
- Wyraża zgodę na dostęp do aplikacji przetwarzających informacje w powierzonym zbiorze danych.
- Wyraża zgodę na udostępnianie informacji zgodnie z przepisami prawa.
- Zawiera umowy powierzenia przetwarzania danych osobowych.
- Podejmuje decyzję w sprawie usuwania zbioru danych po konsultacji z IOD.
- Wyznacza Koordynatorów PBI.
- Wyznacza Gospodarza.

2.1.5 Koordynator Polityki Bezpieczeństwa Informacji

- Realizuje postanowienia MAI w zakresie SZBI.
- Świadczy pomoc merytoryczną współpracownikom w zakresie SZBI.
- Inicjuje proces utworzenia i anulowania dostępu do konta w domenie.
- Inicjuje proces o nadanie, modyfikację i anulowanie uprawnień do aplikacji SI UMK.
- Inicjuje proces o nadanie, anulowanie i modyfikowanie upoważnień do przetwarzania danych osobowych.
- Inicjuje proces o nadanie, anulowanie i przedłużenie karty elektronicznej.
- Inicjuje proces o nadanie, anulowanie i modyfikowanie dostępu do pomieszczeń.
- Inicjuje proces o nadanie, anulowanie i modyfikowanie konta e-mail.
- Inicjuje proces o nadanie, anulowanie i modyfikowanie podpisu elektronicznego.
- Współpracuje z IOD i Gospodarzem.
- Odpowiada za kompletność informacji zamieszczonych w Systemie Ewidencjonowania Zbiorów, Administrowania i Monitorowania w zakresie kompetencji swoich komórek oraz za aktualność tych danych.

- Współpracuje przy dokumentowaniu SZBI.
- Uczestniczy w opracowaniu, testowaniu oraz utrzymaniu PCD.

2.1.6 Administrator Techniczny

- Odpowiada za właściwą konfigurację i administrowanie elementami SI UMK, w szczególności za zapewnienie bezpieczeństwa przetwarzania informacji.
- Odpowiada za bieżące monitorowanie elementów SI UMK, w szczególności pod kątem prób nieautoryzowanego dostępu do informacji chronionych.
- Przeciwdziała próbom włamania, zniszczenia oraz nieautoryzowanego dostępu do elementów SI UMK, w tym także do informacji chronionych.
- Odpowiada za techniczne udostępnianie informacji chronionych na wniosek MAI, jeżeli użytkownik nie ma uprawnień bądź możliwości.
- Odpowiada za tworzenie i zabezpieczenie kopii zapasowych danych chronionych oraz zasobów lub konfiguracji elementów SI UMK, niezbędnych do prawidłowej pracy SI UMK lub do przetwarzania danych chronionych.
- Prowadzi ewidencję użytkowników elementów SI UMK oraz technicznie nadaje uprawnienia użytkownikom zaakceptowanym przez MAI.
- Realizuje asystę techniczną elementów SI UMK.
- Prowadzi dokumentację techniczną elementów SI UMK.
- Prowadzi nadzór kondycji eksploatowanego sprzętu komputerowego oraz rekomenduje potrzeby w zakresie jego modernizacji, zakupu i wycofania z użytku.
- Przeprowadza okresowe przeglądy kont i uprawnień użytkowników w aplikacjach.
- Wnioskuję do odpowiedniego MAI o cofnięcie uprawnień użytkownikowi, który wykorzystał je w sposób niewłaściwy i jednocześnie zgłasza incydent bezpieczeństwa do IOD.
- Podejmuje natychmiastowe działania zabezpieczające w przypadku zagrożenia bezpieczeństwa SI UMK i jednocześnie zgłasza incydent bezpieczeństwa do AS i IOD.
- Prowadzi bieżącą współpracę z użytkownikami SI UMK w zakresie poprawnego działania bezpośrednio używanych elementów SI.

2.1.7 Gospodarz

- Koordynuje przetwarzanie danych w aplikacji przez użytkowników SI UMK.
- Kontroluje i aktualizuje słowniki aplikacji.
- Prowadzi szkolenia dla nowych użytkowników aplikacji.
- Współpracuje z AT w zakresie merytorycznym i technicznym pracy aplikacji.
- Wnioskuję do AS o dokonanie zmian w aplikacji usprawniających pracę użytkowników.
- Wnioskuję do AS o dostosowanie aplikacji do zmian w przepisach prawa prawnych oraz w strukturze organizacyjnej UMK.
- W uzasadnionych przypadkach dla wskazanych przez AS Aplikacji, w zastępstwie prowadzi ewidencję użytkowników Aplikacji SI UMK oraz technicznie nadaje uprawnienia użytkownikom zaakceptowanym przez MAI.

2.1.8 Pozostałe odpowiedzialności

Za opracowywanie i aktualizację procedur, instrukcji, regulaminów i in. dokumentów w obszarach SZBI odpowiadają:

- Obszar bezpieczeństwa prawo-organizacyjnego – kierujący komórką organizacyjną właściwą dla spraw organizacji i nadzoru pracy UMK,
- Obszar bezpieczeństwa zasobów ludzkich - kierujący komórką organizacyjną właściwą dla spraw personalnych UMK,
- Obszar bezpieczeństwa fizycznego - kierujący komórką organizacyjną właściwą dla spraw obsługi UMK,
- Obszar bezpieczeństwa teleinformatycznego – kierujący komórką organizacyjną właściwą dla spraw informatyki UMK.

W innych przypadkach osoby odpowiedzialne za opracowywanie, zatwierdzanie i aktualizację procedur, instrukcji, regulaminów i in. dokumentów wskazuje IOD.

2.2 Zarządzanie zbiorami danych

Rozdział wprowadza wymagania w zakresie bezpieczeństwa zbiorów informacji przetwarzanych w UMK, reguluje kwestię tworzenia, aktualizacji, usuwania, udostępniania zbiorów informacji chronionych w UMK oraz zbiorów informacji szczególnie chronionych w postaci zbiorów danych osobowych. Zawiera w szczególności wykaz zbiorów, opis struktury danych, opis przepływu danych, środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i dostępności danych. Szczegółowo opisuje wymagania dotyczące powierzania, udostępniania danych, realizacji prawa osoby, której dane dotyczą, zarządzania upoważnieniami do przetwarzania danych osobowych.

2.2.1 Udostępnianie informacji chronionych

- 1) Decyzję o udostępnieniu danych chronionych podejmuje MAI. W zależności od rodzaju informacji udostępniane są w formie:
 - a) telefonicznej,
 - b) na pisemny wniosek,
 - c) do wglądu,
 - d) poprzez pocztę elektroniczną,
 - e) poprzez strony internetowe (www.bip.krakow.pl, www.krakow.pl),
 - f) na tablicach ogłoszeń,
 - g) w innej formie, określonej przepisem prawa.
- 2) Informacje chronione udostępniane są na zasadach określonych przepisami prawa.

2.2.2 Udostępnianie danych osobowych

- 1) Dane osobowe udostępnia się na pisemny, umotywowany wniosek (formularz F-2) chyba, że przepis prawa stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.
- 2) Wniosek składa się do MAI.

- 3) Wszystkie wnioski rejestrowane są u właściwego MAI.
- 4) MAI rozpatruje wniosek pod kątem spełnienia wymagań formalnych. W szczególności sprawdza czy wniosek zawiera:
 - a) dane o wnioskodawcy,
 - b) zakres żądanych informacji,
 - c) cel pozyskania danych,
 - d) podstawę prawną upoważniającą do pozyskania informacji albo wiarygodne uzasadnienie potrzeby posiadania danych.
- 5) Jeśli wniosek nie zawiera któregoś z powyżej wskazanych elementów, wnioskodawcę wzywa się do uzupełnienia wniosku.
- 6) Przed udostępnieniem danych wnioskodawca podpisuje Oświadczenie o ochronie udostępnionych danych osobowych – formularz F-3, jeżeli przepisy szczególne nie regulują obowiązków związanych z przetwarzaniem danych osobowych przez tego odbiorcę.
- 7) MAI jest zobowiązany dokumentować każdą sprawę związaną z realizacją wniosku zgodnie z Instrukcją kancelaryjną dla organów gmin i związków międzygminnych.

2.2.3 Realizacja praw osoby, której dane dotyczą

- 1) Spełnienie praw osoby, której dane dotyczą obejmuje:
 - a) udzielenie informacji w zakresie określonym w art. 12 RODO,
 - b) dokonanie uzupełnienia, uaktualnienia, sprostowania danych osobowych w zbiorach danych osobowych,
 - c) wstrzymanie przetwarzania danych osobowych.
- 2) Spełnienie praw osoby wymaga złożenia do MAI pisemnego wniosku, precyzującego żądanie Wnioskodawcy.
- 3) Decyzję o realizacji żądań zawartych we wniosku podejmuje MAI. Następuje to w formie pisemnej.
- 4) MAI zobowiązany jest rozpatrzyć i zrealizować wniosek niezwłocznie, najpóźniej w terminie miesiąca od dnia wpływu wniosku do UMK.

2.2.4 Zarządzanie upoważnieniami do przetwarzania danych osobowych

- a) Do przetwarzania danych osobowych mogą być dopuszczone tylko osoby posiadające ważne upoważnienie do przetwarzania danych osobowych (formularz F- 1) w zbiorze danych osobowych UMK oraz w zbiorach danych osobowych powierzonych UMK w ramach zawartych umów.
- b) Upoważnienia do przetwarzania danych osobowych w UMK wydaje AD lub osoba działająca z upoważnienia AD. Upoważnienia wydaje się na wniosek kierującego komórką organizacyjną UMK.

2.3 Bezpieczeństwo w kontaktach ze stronami trzecimi

Bezpośredni dostęp do istotnych aktywów UMK przez strony trzecie, ze szczególnym uwzględnieniem dostępu do zasobów informacyjnych, wymaga zobowiązania strony zewnętrznej do podpisania oświadczenia o zachowaniu poufności F-29.

Strony trzecie uzyskujące dostęp do istotnych aktywów, to w szczególności:

- a) zespoły wsparcia oraz serwisowania sprzętu i oprogramowania,
- b) stażyści i praktykanci,
- c) osoby zatrudnione na umowę o dzieło lub umowę zlecenia,
- d) miejskie jednostki organizacyjne,
- e) instytucje zewnętrzne.

3. Bezpieczeństwo teleinformatyczne

Poprzez termin „bezpieczeństwo teleinformatyczne” rozumie się odpowiednie zarządzanie SI UMK, kontrolę dostępu do SI UMK oraz jego zasobów, a także pozyskiwanie, rozwój i utrzymywanie aplikacji. W tym rozdziale szczegółowo opisany jest SI UMK, jego zabezpieczenia oraz zasady eksploataowania.

3.1 Instrukcja zarządzaniem SI UMK

Instrukcja zarządzania SI UMK ustanawia ogólne zasady dla SI UMK oraz wspólne procedury dla jego elementów. Jeżeli dla poszczególnych składników SI UMK regulacje są inne niż w Instrukcji zarządzania SI UMK, wówczas sporządza się szczegółowe instrukcje zarządzania danym elementem SI UMK, stanowiące dokumenty komplementarne do niniejszego rozdziału. Każda szczegółowa instrukcja powinna zawierać co najmniej:

- a) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności,
- b) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem,
- c) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu,
- d) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania,
- e) sposób, miejsce i okres przechowywania:
 - elektronicznych nośników informacji zawierających dane osobowe,
 - kopii zapasowych, o których mowa w lit. d),
- f) sposób zabezpieczenia SI UMK przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu,
- g) sposób odnotowania informacji o odbiorcach danych (w rozumieniu art. 4 pkt 9 RODO), którym dane osobowe zostały udostępnione oraz dacie i zakresie tego udostępnienia,
- h) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

3.2 Zarządzanie upoważnieniami i uprawnieniami

Zasady nadawania, zmiany i odbierania upoważnień do przetwarzania danych osobowych oraz uprawnień do aplikacji.

3.2.1 Uprawnienia do pracy w SI UMK dla stron trzecich:

- 1) Dostęp do SI UMK oraz do aplikacji SI UMK mogą posiadać także strony trzecie:

- a) pracownicy miejskich jednostek organizacyjnych,
 - b) pracownicy podmiotów, z którymi zawarto odrębne umowy (np. umowy o świadczenie usługi wsparcia technicznego),
 - c) inne osoby zewnętrzne.
- 2) Strony trzecie ubiegające się o dostęp do SI UMK muszą przedłożyć w formie pisemnej odpowiedni wniosek, którego wzór przedstawiono na formularzu F-11. Wniosek podpisuje osoba upoważniona do składania oświadczeń w imieniu strony trzeciej.
 - 3) Miejska jednostka organizacyjna lub 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 realizowany jest przez koordynatora PBI właściwego Wydziału, który inicjuje odpowiedni proces w SEZAM.
 - 6) Dostęp do SI UMK lub do aplikacji SI UMK dla stron trzecich może być przyznany wyłącznie na czas określony nie dłuższy niż czas trwania umowy zawartej z Gminą Miejską Kraków. Pracownicy miejskich jednostek organizacyjnych, mogą uzyskać dostęp do SI UMK na okres wskazany we wniosku F-11, jednak nie może on przekraczać terminu zatrudnienia w miejskiej jednostce. W pozostałych przypadkach o terminie przyznania dostępu do SI UMK decyduje AS.
 - 7) Przedłużenie dostępu do SI UMK uzyskuje się po zainicjowaniu procesu modyfikacji konta w domenie/modyfikacja upoważnienia (uprawnienia), przy czym okres, na jaki przedłuża się dostęp nie może być dłuższy niż określony w pkt. 6).
 - 8) Odebranie uprawnień do SI UMK następuje:
 - a) automatycznie po upływie okresu, na jaki przyznano upoważnienia (uprawnienia),
 - b) na wniosek strony trzeciej,
 - c) decyzją IOD lub AS, AC
 - 9) Przed otrzymaniem dostępu do SI UMK każda osoba musi podpisać oświadczenie o zachowaniu poufności F-29.
 - 10) Oryginały podpisanych oświadczeń o zachowaniu poufności F-29 oraz zgłoszonych wniosków przez strony trzecie F-11 przechowywane są u Koordynatorów PBI w komórkach organizacyjnych UMK.
 - 11) Rejestr Oświadczeń o zachowaniu poufności F-29 prowadzony jest w wersji elektronicznej w aplikacji SEZAM.
 - 12) W szczególnych przypadkach - w celu zapewnienia ciągłości działania SI UMK, AS - na wniosek właściwego AT może wyrazić zgodę na dostęp do SI UMK dla stron trzecich bez formalnego podpisania umowy; w tym przypadku wyrażenie zgody przez AS jest podstawą do uruchomienia odpowiedniego procesu w SEZAM. Procedura taka nie zwalnia z konieczności wypełnienia przez ww. stronę trzecią Formularza F-29 i F-11.
 - 13) Dostęp w trybie opisanym w pkt. 12) może zostać udzielony na maksymalnie 30 dni kalendarzowych, nie może zostać przedłużony bez formalnej umowy (z procedury tej można skorzystać wyłącznie w odniesieniu do strony trzeciej, która współpracowała już z UMK na podstawie umów).

3.2.2 Uprawnienia do pracy zdalnej w SI UMK:

- 14) Wszystkie osoby posiadające uprawnienia do pracy w SI UMK lub ubiegające się

- o takie uprawnienia mogą posiadać dostęp zdalny do SI UMK za pomocą:
- a) technologii VPN (możliwy dostęp do wszystkich aplikacji),
 - b) innych technologii, np. za pomocą przeglądarki internetowej (możliwy dostęp do wybranych aplikacji).
- 15) Rejestr wszystkich osób, którym przyznano zdalny dostęp do SI UMK za pomocą technologii VPN jest prowadzony w SEZAM, jako wykaz upoważnień do aplikacji „Zdalny dostęp”.
- 16) Dostęp zdalny do SI UMK za pomocą innych technologii (np. przeglądarki internetowej) do wybranych aplikacji jest przyznawany za pośrednictwem SEZAM po zainicjowaniu procesu o nadanie uprawnienia w tych aplikacjach i uzyskaniu akceptacji oraz nie jest ewidencjonowany w SEZAM, jako „Zdalny dostęp”.

5.1.1 Konto użytkownika w SI UMK

- 1) Dla każdego użytkownika SI UMK – AT ustala odrębny identyfikator użytkownika.
- 2) Każdy użytkownik SI UMK może posiadać tylko jeden identyfikator użytkownika taki sam dla wszystkich posiadanych kont w SI UMK. Nie można zmieniać tego identyfikatora lub przyznawać takiego samego identyfikatora innemu użytkownikowi,
- 3) pod warunkiem, iż żaden z używanych przez niego identyfikatorów użytkownika nie jest używany przez innego użytkownika SI UMK.
- 4) AS nadzoruje ewidencję wszystkich przyznaczonych identyfikatorów użytkownika w SI UMK.
- 5) Konto użytkownika może być wykorzystywane przez użytkownika wyłącznie do realizacji powierzonych zadań. W szczególności nie może być ono wykorzystywane do rozpowszechniania treści i obrazów wulgarnych, obrażających osoby trzecie, naruszających czyjekolwiek dobra osobiste lub niezgodnych z prawem.
- 6) W przypadku utraty hasła użytkownik zobowiązany jest zgłosić się niezwłocznie do odpowiedniego AT.
- 7) Hasła użytkownika utrzymuje się w tajemnicy, również po upływie ich ważności.
- 8) AT blokuje konto użytkownika, który niewłaściwie chroni swoje hasło lub wykorzystuje je niezgodnie z postanowieniami niniejszej instrukcji.

5.1.2 Odpowiedzialność użytkownika

- 1) Użytkownikiem jest każda osoba, która uzyskała dostęp do SI UMK.
- 2) Użytkownik jest odpowiedzialny za:
 - a) niezwłoczne poinformowanie o nieautoryzowanym dostępie do informacji chronionych na adres Inspektora Ochrony Danych UMK iod@um.krakow.pl,
 - b) zachowanie w tajemnicy wszelkich posiadanych haseł chroniących jego konta użytkownika w SI UMK,
 - c) wykorzystywanie posiadanych identyfikatorów użytkownika wyłącznie do realizowanych zadań,
 - d) prawidłowe korzystanie z aplikacji zgodnie z powierzonymi obowiązkami,
 - e) 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.

5.1.3 Ochrona haseł

- 1) Użytkownik ponosi pełną odpowiedzialność za powierzone mu lub utworzone przez niego hasła oraz za ich przechowywanie.
- 2) Hasła użytkowników lub inne dane uwierzytelniające podlegają szczególnej ochronie.
- 3) Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu hasła, które jest związane z jego identyfikatorem.
- 4) Każdy użytkownik posiadający dostęp do SI UMK zobowiązany jest do:
 - a) niezwłocznej zmiany hasła tymczasowego, przekazanego przez AT,
 - b) niezwłocznej zmiany hasła w przypadkach zaistnienia podejrzenia lub rzeczywistego ujawnienia hasła
 - c) poinformowania IOD UMK o podejrzeniu lub rzeczywistym ujawnieniu hasła,
 - d) stosowania hasła, które:
 - składa się z minimum 12 znaków,
 - zawiera małe litery,
 - zawiera duże litery,
 - zawiera cyfry,
 - zawiera znaki specjalne,
 - jest inne niż 10 ostatnio wprowadzonych haseł,
 - e) zmiany wykorzystywanych haseł w regularnych odstępach czasu (raz na 90 dni).
- 5) Użytkownikowi zabrania się:
 - a) używania tych samych haseł w różnych elementach SI UMK (oprogramowanie systemowe, aplikacje, elementy sieci komputerowej itp.),
 - b) zapisywania haseł w sposób jawny i umieszczania ich w miejscach dostępnych dla innych osób, oraz przechowywania listy haseł na swoim komputerze w postaci tekstu.
 - c) stosowania haseł opartych na skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby, np. imiona, numery telefonów, daty urodzenia itp.,
 - d) udostępniania haseł innym użytkownikom.

4. Formularze:

4.1 F-11 Wzór wniosku o przyznanie dostępu do SI UMK.

4.2 F-29 Oświadczenie o zachowaniu poufności dla stron trzecich.

F-11 Wzór wniosku o przyznanie dostępu do SI UMK

ID	Wersja	Data	Nazwa	Zatwierdziła
F-11	6.0	25.10.2024	Wzór wniosku o przyznanie dostępu do SI UMK	Renata Woyciechowska - IOD
Formularz do procedury D-1				

Kraków, dnia

.....

Imię i nazwisko osoby wypełniającej wniosek

.....

Nazwa strony trzeciej

WNIOSEK O PRYZNANIE DOSTĘPU DO SI UMK

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

.....
(numer umowy, podstawa prawna)

W celu:

.....

dla następujących osób:

LP.	Imię i Nazwisko	PESEL	Adres poczty elektronicznej	Numer telefonu
1.				
2.				
3.				

Dane teleadresowe strony trzeciej:

Pełna nazwa strony trzeciej:

Nazwa skrócona:

NIP:

REGON:

Dane kontaktowe (tel., e-mail):

Adres siedziby firmy:

.....

Adres korespondencyjny:

.....

Dostęp do danych osobowych: TAK/NIE*:

(Treść tabeli należy uzgodnić z osobą odpowiedzialną w UMK za realizację umowy/zadania)

LP.	Nazwa zbioru danych	Nazwa aplikacji	Nazwa roli w aplikacji

Dostęp ma być przyznany:

- na okres od..... do
- bezterminowo

Lista zadań przewidzianych do realizacji w SI UMK:

1.

.....

2.

.....

Działając w imieniu

(nazwa strony trzeciej)

oświadczam, że zobowiązuje się do pokrycia wszelkich szkód spowodowanych przez działanie osób uzyskujących dostęp do SI UMK, w szczególności kosztów usuwania uszkodzeń SI UMK powstałych w wyniku naruszenia przepisów, regulacji i zobowiązań wskazanych w pkt. I Oświadczenia o zachowaniu poufności dla stron trzecich.

Zobowiązuję się do natychmiastowego powiadomienia Inspektora Ochrony Danych UMK, pisemnie lub pocztą elektroniczną na adres: iod@um.krakow.pl o odebraniu uprawnień dla zgłoszonych pracowników w przypadku, gdy dostęp do SI UMK utracił zasadność (np. zmiana zakresu obowiązków, ustanie stosunku pracy itp.).

.....

Czytelny podpis osoby upoważnionej do składania wniosku w imieniu strony trzeciej

** niepotrzebne skreślić*

INFORMACJA ADMINISTRATORA O PRZETWARZANIU DANYCH OSOBOWYCH
dla osób mających uzyskać dostęp do Systemu Informatycznego Urzędu Miasta
Krakowa, których dane osobowe zawarto we wniosku

Zgodnie z art. 14 ust. 1 i 2 unijnego ogólnego rozporządzenia o ochronie danych (tzw. RODO) informujemy, że administratorem danych osobowych jest Prezydent Miasta Krakowa z siedzibą Pl. Wszystkich Świętych 3-4, 31-004 Kraków. Z administratorem można się skontaktować listownie (adres jw.) lub drogą elektroniczną – adres e-mail: or.umk@um.krakow.pl.

Dane osobowe będą przetwarzane w celu prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych w Systemie Informatycznym Urzędu Miasta Krakowa. Dane są objęte rejestrem czynności przetwarzania pn. UŻYTKOWNICY SYSTEMU INFORMATYCZNEGO UMK.

Informujemy, że:

1. Ma Pan/Pani prawo do żądania od administratora dostępu do swoich danych osobowych, ich sprostowania, ograniczenia przetwarzania.
2. Dane osobowe będą przetwarzane do czasu ustania uprawnień dostępu do Systemu Informatycznego Urzędu Miasta Krakowa, a następnie są archiwizowane, ale nie usuwane.
3. Ma Pan/Pani prawo do wniesienia skargi w związku z przetwarzaniem danych do organu nadzorczego, którym jest Prezes Urzędu Ochrony Danych Osobowych.
4. Dane osobowe są pozyskiwane od jednostki składającej wniosek o przyznanie dostępu do Systemu Informatycznego Urzędu Miasta Krakowa.
5. Zgodnie z wymogiem ustawowym oraz naszymi wewnętrznymi regulacjami, wymagamy podania danych osobowych, które są niezbędne do nadania uprawnień w systemie informatycznym, aby móc wykonać swoje obowiązki. Konsekwencją niepodania danych jest brak możliwości nadania uprawnień do pracy w Systemie Informatycznym Urzędu Miasta Krakowa.
6. Podstawę prawną przetwarzania danych stanowi ustawa z dnia 8 marca 1990 r. o samorządzie gminnym, ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym,

ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne i rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

Ponadto informujemy, że ma Pan/Pani prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania swoich danych osobowych, z przyczyn związanych z Pana/Pani szczególną sytuacją.

Dane kontaktowe Inspektora Ochrony Danych: adres pocztowy – jw., adres e-mail:
iod@um.krakow.pl

F-29 Oświadczenie o zachowaniu poufności dla stron trzecich

ID	Wersja	Data	Nazwa	Zatwierdziła
F-29	4.0	07.11.2023	Oświadczenie o zachowaniu poufności dla stron trzecich	Renata Woyciechowska – IOD UMK
Formularz do procedury D-1				

.....
(Imię i nazwisko)

Kraków, dnia

.....
(Nazwa strony trzeciej)

OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI

1. Niniejszym oświadczam, że:

- a) Zapoznałam (-em) się z obowiązującymi w Polsce przepisami dotyczącymi ochrony danych osobowych;
- b) Zapoznałam (-em) się z regulacjami obowiązującymi w Urzędzie Miasta Krakowa dotyczącymi Systemu Zarządzania Bezpieczeństwem Informacji.

Zobowiązuję się do przestrzegania powyższych przepisów i regulacji zarówno w trakcie wykonywania zadań, w związku z przyznanymi uprawnieniami, jak i po ich ustaniu.

Zobowiązuję się ponadto do zachowania w tajemnicy informacji poufnych oraz do niewykorzystywania ich dla innych celów niż te, dla których dostęp do aktywów Urzędu Miasta Krakowa został mi przyznany. Za informacje poufne rozumie się wszelkie informacje, które nie są znane lub nie powinny być znane publicznie, a w szczególności informacje stanowiące tajemnice prawem chronione, w tym informacje chronione na podstawie przepisów o ochronie danych osobowych.

Obowiązek zachowania w tajemnicy informacji poufnych trwa przez okres wynikający z umowy zawartej przez Gminę Miejską Kraków, a w przypadku miejskich jednostek organizacyjnych – przez okres zatrudnienia w jednostce i okres 3 lat po zakończeniu zatrudnienia.

2. Przyjmuję do wiadomości, iż:

- a) moje działania w Urzędzie Miasta Krakowa mogą być rejestrowane oraz monitorowane;
- b) postępowanie sprzeczne z niniejszym oświadczeniem może być uznane za naruszenie bezpieczeństwa danych osobowych w rozumieniu przepisów o ochronie danych osobowych;

- c) w przypadku poniesienia szkody przez Urząd Miasta Krakowa, wynikających z naruszenia przeze mnie przepisów, regulacji i zobowiązań wskazanych w pkt. 1, Urząd Miasta Krakowa może dochodzić roszczeń na drodze sądowej.

.....
(czytelny podpis)