

**Procedura zarządzania uprawnieniami,
zasady zarządzania zmianą oraz zasady zgłaszania błędów aplikacji
Zintegrowany System Zarządzania Nieruchomościami „Granit”.**

I. Podstawa prawna.

- I.1. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U z 2002 r. Nr 101, poz. 926 z późn. zm.)
- I.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)

II. Definicje i skróty.

Ilekcroć w niniejszej procedurze jest mowa o:

- | | |
|--------------------------------|---|
| 1) ZSZN | – Zintegrowany System Zarządzania Nieruchomościami GRANIT |
| 2) Użytkownik | – każda osoba posiadająca dostęp do ZSZN |
| 3) ABI | – Administrator Bezpieczeństwa Informacji w ZBK |
| 4) ASI | – Administrator Systemu Informatycznego w ZBK |
| 5) AT | – Administrator Techniczny ZSZN w UMK |
| 6) KPBI | – Koordynator Polityki Bezpieczeństwa Informacji w UMK |
| 7) SI | – System Informatyczny |
| 8) UMK | – Urząd Miasta Krakowa |
| 9) systemowa nazwa użytkownika | – login nadany użytkownikowi w Systemie Informatycznym ZBK, a w Systemie Informatycznym UMK - identyfikator użytkownika |
| 10) ZBK | – Zarząd Budynków Komunalnych w Krakowie |
| 11) Wykonawca | – podmiot świadczący umowę asysty technicznej dla aplikacji ZSZN |
| 12) Wydział | – rozumie się przez to również komórkę organizacyjną UMK na prawach Wydziału |

III. Zakres przedmiotowy.

Procedura określa zasady:

- nadawania, zmiany i odbierania upoważnień do przetwarzania danych osobowych w aplikacji ZSZN,
- nadawania, zmiany i odbierania dostępu do SI ZBK, SI UMK oraz uprawnień do aplikacji ZSZN,
- zarządzania zmianą aplikacji ZSZN,
- zgłaszania błędów aplikacji ZSZN.

IV. Zasady nadawania, zmiany i odbierania upoważnień do przetwarzania danych, dostępu do SI ZBK, SI UMK oraz uprawnień do aplikacji ZSZN.

Listę administratorów ZSZN prowadzi na bieżąco ABI, który w przypadku zmian na tej liście przesyła drogą e-mailową zaktualizowaną listę do AT oraz KPBI.

IV.1. Zasady nadawania, zmiany i odbierania upoważnień do przetwarzania danych, dostępu do SI ZBK oraz uprawnień do aplikacji ZSZN w części pozostającej w gestii ZBK.

IV.1.1. Nadawanie upoważnień dla pracowników ZBK.

Kierownik komórki organizacyjnej ZBK występuje do ABI o nadanie, zmianę zakresu i uchylenie upoważnienia do przetwarzania danych dla podległego mu pracownika. Szczegółowy tryb nadawania, zmiany i uchylania uprawnień określony jest w obowiązującej Polityce Bezpieczeństwa Informacji ZBK oraz Instrukcji Zarządzania Systemami Informatycznymi ZBK.

IV.1.2. Zasady nadawania i odbierania upoważnień do przetwarzania danych, dostępu do SI ZBK oraz uprawnień do aplikacji ZSZN w części pozostającej w gestii ZBK, dla osób nie będących pracownikami ZBK.

Dostęp do SI ZBK lub do aplikacji ZSZN w części pozostającej w gestii ZBK dla osób nie będących pracownikami ZBK może być przyznawany wyłącznie na czas określony, nie dłuższy niż 12 miesięcy.

IV.1.2.1. Nadanie dostępu

IV.1.2.1.1. Podmiot zainteresowany dostępem do SI ZBK występuje do ABI o umożliwienie dostępu dla wskazanej osoby. Wzór wniosku stanowi załącznik nr 1 niniejszej procedury.

We wniosku należy wskazać imię i nazwisko osoby, jej systemową nazwę użytkownika oraz dane kontaktowe, a także dane podmiotu, który składa wniosek.

IV.1.2.1.2. Osoba starająca się o dostęp zobowiązana jest do zapoznania się i podpisania oświadczenia o zachowaniu poufności. Przedmiotowe oświadczenie stanowi załącznik nr 2 do niniejszej procedury.

IV.1.2.1.3. ASI nadaje hasło do SI ZBK i uprawnienia do korzystania z ZSZN w części pozostającej w gestii ZBK.

IV.1.2.1.4. ABI, po utworzeniu konta użytkownika w SI ZBK, informuje o powyższym przesyłając wiadomość e-mail zawierającą nr telefonu i adres e-mail ASI, na odpowiednie konto podmiotu wskazane we wniosku o nadanie dostępu.

IV.1.2.1.5. Uprawniona osoba telefonicznie zgłasza się do ASI po odbiór hasła do SI ZBK oraz hasła do aplikacji ZSZN. Użytkownik po otrzymaniu hasła do SI ZBK ma obowiązek dostosowywania go do swojego hasła domenowego.

IV.1.2.2. Przedłużenie dostępu

Przedłużenie dostępu następuje na wniosek podmiotu zainteresowanego dostępem do SI ZBK (załącznik nr 1 do niniejszej procedury) i po złożeniu przez niego oświadczenia, o którym mowa w pkt IV.1.2.1.2 (załącznik nr 2 do niniejszej procedury).

Wniosek wraz z oświadczeniem winien być złożony na minimum 14 dni przed upływem terminu, na jaki dostęp został przyznany.

IV.1.2.3. Odebranie dostępu

Odebranie dostępu następuje:

- automatycznie po upływie terminu, na jaki dostęp został przyznany,
- na pisemny wniosek podmiotu posiadającego dostęp do SI ZBK, skierowany do ABI.

IV.2. Zasady nadawania, zmiany i odbierania upoważnień do przetwarzania danych, dostępu do SI UMK, SI ZBK oraz uprawnień do aplikacji ZSZN w części pozostającej w gestii UMK.

Praca w aplikacji ZSZN w części pozostającej w gestii UMK jest możliwa dopiero po uzyskaniu dostępu do SI ZBK.

Dostęp do SI ZBK dla osób nie będących pracownikami ZBK przyznawany jest zgodnie z zasadami opisanymi w pkt IV.1.2.

IV.2.1. Zasady nadawania, zmiany i odbierania upoważnień do przetwarzania danych, dostępu do SI UMK, SI ZBK oraz uprawnień do aplikacji ZSZN w części pozostającej w gestii UMK dla osób z UMK.

Upoważnienia do przetwarzania danych, dostępu do SI UMK i uprawnień do aplikacji ZSZN w części pozostającej w gestii UMK dla osób z UMK określone są w obowiązującym zarządzeniu Prezydenta Miasta Krakowa w sprawie wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Krakowa, Procedurą zarządzania upoważnieniami i uprawnieniami - D-1 oraz przy uwzględnieniu poniższych zapisów:

- KPBI z zainteresowanego Wydziału UMK informuje za pośrednictwem wiadomości e-mail AT oraz uprawnioną osobę o otrzymaniu dostępu do

SI ZBK,

- AT przyznaje dostęp do aplikacji ZSZN, zgodnie z przyznanym upoważnieniem i przekazuje użytkownikowi hasło do aplikacji ZSZN.

IV.2.2. Zasady nadawania, zmiany i odbierania upoważnień do przetwarzania danych, dostępu do SI UMK, SI ZBK oraz uprawnień do aplikacji ZSZN w części pozostającej w gestii UMK dla osób trzecich.

Dostęp do SI UMK i upoważnienia do aplikacji ZSZN w części pozostającej w gestii UMK dla osób trzecich określone są w obowiązującym zarządzeniu Prezydenta Miasta Krakowa w sprawie wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Krakowa oraz przy uwzględnieniu poniższych zapisów:

- KPBI z zainteresowanego Wydziału UMK informuje za pośrednictwem wiadomości e-mail AT oraz uprawnioną osobę o otrzymaniu dostępu do SI ZBK,
- AT przyznaje dostęp do aplikacji ZSZN, zgodnie z przyznanym upoważnieniem i przekazuje użytkownikowi hasło do aplikacji ZSZN.

Wzór oświadczenia o zachowaniu poufności oraz wzór wniosku o przyznanie dostępu do SI UMK stanowią załączniki do obowiązującego zarządzenia Prezydenta Miasta Krakowa w sprawie wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Krakowa.

Zasady zarządzania bezpieczeństwem informacji w UMK są udostępniane przez KPBI zainteresowanego Wydziału UMK na wniosek osoby zainteresowanej dostępem.

V. Zasady zarządzania zmianą aplikacji ZSZN

- V.1. W przypadku udostępnienia na stronie internetowej Wykonawcy nowej poprawki do aplikacji ZSZN, Koordynator ZSZN powiadamia telefonicznie lub mailowo wyznaczone osoby o zaistniałym fakcie oraz ustala najbliższy możliwy termin instalacji poprawki nie kolidujący z normalną pracą aplikacji ZSZN. Lista osób, które należy poinformować, stanowi załącznik nr 3 do niniejszej procedury.
- V.2. W przypadku wyrażenia przez osoby wymienione w załączniku nr 3 do niniejszej procedury zgody na wgranie poprawki, Koordynator ZSZN ustala datę i czas planowanej instalacji poprawki z ASI.
O powyższym osoby te poinformowane zostaną drogą telefoniczną lub e-mailową.
- V.3. W przypadku, gdy którakolwiek z osób wymienionych w załączniku nr 3 do niniejszej procedury nie wyrazi zgody na instalację poprawki, Koordynator ZSZN poinformuje pozostałe osoby o zaistniałym fakcie oraz wstępnie ustali prawdopodobną datę ponownej próby instalacji.
- V.4. Instalacja poprawki odbywa się po godzinach pracy i wykonywana jest przez ASI. W przypadkach błędów krytycznych, możliwa jest instalacja poprawki w trakcie godzin pracy jednostek po wcześniejszym uzgodnieniu niniejszego z osobami wymienionymi w załączniku nr 3 do niniejszej procedury oraz podjęciu wszystkich wymaganych kroków w celu zabezpieczenia aplikacji ZSZN przed awarią.
- V.5. Przed instalacją poprawki tworzona jest przez ASI zapasowa kopia bezpieczeństwa-

aplikacji ZSZN oraz bazy danych.

- V.6. Koordynator ZSZN informuje osoby wymienione w załączniku nr 3 do niniejszej procedury o wyniku przeprowadzonej instalacji drogą e-mailową lub telefoniczną. W przypadku blokady aplikacji ZSZN, Koordynator ZSZN, po otrzymaniu informacji od Wykonawcy, poinformuje również osoby wymienione w załączniku nr 3 do niniejszej procedury o przewidywanej dacie (godzinie) usunięcia blokady.
- V.7. Zawartość poprawek jest opisana i umieszczana na stronie internetowej Wykonawcy i dostępna dla wszystkich użytkowników aplikacji ZSZN.

VI. Zasady zgłaszania błędów aplikacji ZSZN.

VI.1. Dla pracowników ZBK.

- VI.1.1. Zgłoszenie błędu następuje wyłącznie drogą e-mailową, od kierownika właściwej komórki organizacyjnej ZBK lub osoby przez niego upoważnionej, do Koordynatora ZSZN.
- VI.1.2. Każdorazowe zgłoszenie powinno składać się z minimum trzech elementów:
- raportu z błędu wygenerowanego przez aplikację ZSZN, ewentualnie zrzutu ekranu ze wskazaniem błędu,
 - opisu w jakiej sytuacji występuje błąd,
 - ścieżki dostępu do miejsca w aplikacji ZSZN gdzie wystąpił błąd.
- VI.1.3. Kompletnie zgłoszenie zostanie przeanalizowane przez Koordynatora ZSZN, który następnie podejmie dalsze działania celem wyeliminowania błędu.
- VI.1.4. Po wyjaśnieniu błędu, czy też zgłoszeniu poprawek do Wykonawcy, zostanie przekazany do zgłaszającego raport o stanie faktycznym.
- VI.1.5. Błędy ewidencjonowane są w postaci elektronicznej.

VI.2. Dla osób nie będących pracownikami ZBK.

- VI.2.1. Zgłoszenie błędu następuje m.in. drogą e-mailową, od Użytkowników aplikacji ZSZN do Gospodarzy ZSZN, wymienionych w załączniku nr 4 do niniejszej procedury.
- VI.2.2. Po weryfikacji błędu przez Gospodarza ZSZN, błędy zgłaszane są drogą e-mailową do jednej z osób upoważnionych w UMK do zgłaszania błędów do Wykonawcy, wymienionych w załączniku nr 5 do niniejszej procedury.
- VI.2.3. Każdorazowe zgłoszenie powinno składać się z minimum trzech elementów:
- raportu z błędu wygenerowanego przez aplikację ZSZN, ewentualnie zrzutu ekranu ze wskazaniem błędu,
 - opisu w jakiej sytuacji występuje błąd,
 - ścieżki dostępu do miejsca w aplikacji ZSZN gdzie wystąpił błąd.
- VI.2.4. Kompletnie zgłoszenie winno być przeanalizowane przez osobę upoważnioną w UMK do zgłaszania błędów do Wykonawcy, wymienioną w załączniku nr 5 do niniejszej procedury, która następnie podejmie dalsze działania celem wyeliminowania błędu.
- VI.2.5. Użytkownikowi zgłaszającemu błąd zostanie wyjaśniony zgłaszany problem lub zostanie przekazana informacja o usunięciu błędu, planowanym terminie jego usunięcia, ewentualnie o innym sposobie pracy w aplikacji ZSZN nie

powodującym powstania takiego błędu.

VII.Przepisy końcowe

VII.1. Aktualizację załączników do niniejszej procedury powierza się Koordynatorowi ZSZN.

VII.2. Poszczególni pracownicy jednostek zobowiązani są do niezwłocznego informowania Koordynatora ZSZN o zaistniałych zmianach personalnych w celu aktualizacji załączników, o których mowa w pkt VII.1.