

## **Załącznik nr 1 do OPZ**

### **Procedura zarządzania uprawnieniami**

#### **1. Cel**

Celem procedury jest określenie sposobu nadawania, zmiany oraz odbierania uprawnień do systemów informatycznych.

#### **2. Zakres**

Procedura dotyczy użytkowników pracujących w systemach informatycznych.

#### **3. Odpowiedzialność**

1. Za aktualizację procedury odpowiedzialny jest ASI
2. Za przestrzeganie procedury odpowiedzialni są:
  - a) użytkownicy systemów informatycznych.
3. Za nadzór nad przestrzeganiem procedury jest:
  - a) Pełnomocnik ds. SZBI.

#### **4. Nadawanie uprawnień**

1. Nadawanie uprawnień następuje na wniosek osoby upoważnionej – Kierownika komórki organizacyjnej bądź IOD.
2. Wyznaczeni pracownicy WSI weryfikują wnioski o nadanie uprawnień.
3. Wniosek o nadanie uprawnień po weryfikacji jego zasadności powinien trafić do akceptacji Sekretarza Miasta, który potwierdza zasadność nadania uprawnień.
4. Wniosek po akceptacji przez Sekretarza Miasta trafia do Prezydenta do akceptacji.
5. Po uzyskaniu akceptacji wniosek trafia do rejestru uprawnień. Wyznaczony pracownik WSI nadaje uprawnienia do systemów. Następnie informuje osobę zainteresowaną o nadanych uprawnieniach oraz przekazuje użytkownikowi identyfikator i hasło.
6. Przydzielenie wskazanych we wniosku uprawnień dla użytkownika odbywa się na odpowiedzialność osoby upoważnionej, która składa wniosek.
7. W przypadku wnioskowania o uprawnienia do systemu, w którym przetwarzane są dane osobowe, wnioskodawca zobowiązany jest do upewnienia się, że użytkownik posiada upoważnienie do przetwarzania danych osobowych.
8. Wniosek o nadanie uprawnień powinien zawierać co najmniej:
  - a) imię i nazwisko pracownika/stażysty/praktykanta,
  - b) nazwę systemu informatycznego wraz z podaniem zakresu uprawnień,
  - c) okres na jaki uprawnienie ma zostać nadane – w przypadku stażysty lub praktykanta.

#### **5. Zmiana uprawnień**

1. Zmiana uprawnień następuje na wniosek Kierownika komórki organizacyjnej, IOD, Pełnomocnika ds. SZBI.
2. Złożenie wniosku o zmianę uprawnienia podlega zasadom, które zostały opisane w pkt. 4 (Nadanie uprawnień)

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

3. Zmiana uprawnień następuje również na podstawie informacji przekazanej z Wydziału Kadr i Rozwoju Personalnego lub osoby upoważnionej do przekazywania informacji kadrowej.
4. Wniosek powinien zawierać co najmniej:
  - a) imię i nazwisko pracownika/stażysty/praktykanta,
  - b) informację czego dotyczy:
    - czasowej nieobecności pracownika (powyżej 1 miesiąca), którą do WSI ma obowiązek zgłaszać Kierownik komórki organizacyjnej,
    - zmiany nazwiska pracownika,
    - zmiany komórki organizacyjnej pracownika,
    - zmiany stanowiska pracownika.
  - c) datę – w przypadku:
    - zmiany komórki organizacyjnej,
    - czasowej nieobecności.
5. Administratorzy (pracownicy WSI) na podstawie otrzymanego wniosku czasowo blokują, zmieniają lub odbierają uprawnienia użytkownikowi.
6. Odblokowanie uprawnień użytkownika czasowo nieobecnego, następuje po jego powrocie do pracy na wniosek bezpośredniego przełożonego lub innej osoby pisemnie upoważnionej. W sytuacji, kiedy zachodzi konieczność odblokowania konta użytkownika w trakcie jego nieobecności lub po zakończeniu zatrudnienia, wniosek taki musi być zgłoszony przez osobę upoważnioną oraz zatwierdzony przez jednego z członków najwyższego kierownictwa (Prezydent, Zastępca Prezydenta, Sekretarz Miasta, Skarbnik Miasta). Dostęp taki musi mieć z góry określony czas, po którym zostanie ponownie zablokowany.

## **6. Odebranie uprawnień**

1. Odebranie uprawnień w trakcie trwającego stosunku pracy lub po jego ustaniu (lub innej umowy np. umowy o staż) następuje na wniosek bezpośredniego przełożonego lub innej osoby pisemnie upoważnionej. Informacja musi być przekazywana bez zbędnej zwłoki.
2. Niezależnie od ustępu 1 Wydział Kadr i Rozwoju Personalnego lub osoba upoważniona informuje Wydział WSI o zwolnieniu pracownika, nie później niż w momencie wystawienia świadectwa pracy.
3. Administratorzy (pracownicy WSI):
  - a) na podstawie otrzymanego wniosku blokują wszystkie uprawnienia wskazanego użytkownika,
  - b) mają prawo zablokować konto użytkownika lub komputera w usłudze katalogowej Active Directory bez dodatkowego powiadamiania, jeżeli nie było ono używane przez okres 1 miesiąca,
  - c) prowadzą ewidencję uprawnień do systemów informatycznych w rejestrze uprawnień.