ZARZĄDZENIE NR 327/19
PREZYDENTA MIASTA SZCZECIN
z dnia 26 lipca 2019 r.

zmieniające zarządzenie w sprawie określenia zasad bezpieczeństwa informacji oraz wytycznych dla Polityki Bezpieczeństwa Informacji Urzędu Miasta Szczecin.

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (Dz. U. z 2019 r. poz. 506 i 1309), art. 24 ust. 1 i 2 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 4.05.2016, s. 1 oraz Dz.Urz. UE L 127 z 23.05.2018, s. 2), art. 1 oraz art. 13 ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2019 r. poz. 700, 730 i 848), **zarządzam, co następuje:**

§ 1. W Zarządzeniu Nr 150/18 Prezydenta Miasta Szczecin z dnia 6 kwietnia 2018 r. w sprawie określenia zasad bezpieczeństwa informacji oraz wytycznych dla Polityki Bezpieczeństwa Informacji Urzędu Miasta Szczecin załącznik Nr 24 Procedura zarządzania uprawnieniami do zasobów/systemów informatycznych Urzędu otrzymuje brzmienie jak w załączniku do zarządzenia.

§ 2. Wykonanie zarządzenia powierza się dyrektorom, kierownikom oraz samodzielnym stanowiskom działającym poza strukturą wydziałów i biur Urzędu Miasta Szczecin.

§ 3. Nadzór nad realizacją zarządzenia powierza się Sekretarzowi Miasta.

§ 4. Zarządzenie wchodzi w życie z dniem 1 sierpnia 2019 r.

Prezydent Miasta

Piotr Krzystek

Załącznik do zarządzenia Nr 327/19

Prezydenta Miasta Szczecin

z dnia 26 lipca 2019 r.

Procedura zarządzania uprawnieniami dostępu do zasobów/systemów informatycznych Urzędu Miasta Szczecin

1. **CEL**

Celem niniejszej procedury jest określenie uporządkowanego, skończonego ciągu czynności procesu zarządzania uprawnieniami, który obejmuje nadawanie, zmianę, przedłużenie oraz odebranie uprawnień pracownikom Urzędu oraz podmiotom zewnętrznym do zasobów i systemów informatycznych Urzędu.

Procedura zarządzania uprawnieniami dostępu do zasobów/systemów informatycznych ma na celu:

1) zapewnienie utrzymania zarządzania poufnością informacji,
2) zapewnienie, że pracownicy Urzędu posiadają odpowiednie poziomy dostępu, umożliwiające wykonywanie ich pracy,
3) zapewnienie redukowania awarii dokonanych przy wprowadzaniu danych lub przy wykorzystaniu usług, przez niewykwalifikowany personel,
4) wprowadzanie możliwości w śledzeniu działania usług oraz ich naruszeń,
5) oferowaniu możliwości ograniczenia dostępów kiedy wymaga tego sytuacja, na określony czas,
6) zapewnienie spójności z wymaganiami prawnymi.

2. **ZAKRES PROCEDURY**

Procedura obejmuje wszystkie jednostki Urzędu oraz podmioty zewnętrzne.

3. **TERMINOLOGIA**

3.1.Wniosek – wniosek dotyczący uprawnień pracownika w formie elektronicznej.

3.2.Właściciel zasobu - jednostka lub podmiot zewnętrzny odpowiedzialny za dostarczanie określonej usługi lub danych w ramach uzgodnionego poziomu jej świadczenia [np. BGM, WSO].

3.3.ASI – Administrator Systemu Informatycznego.

3.4.ASU – Administrator Systemu Użytkowego.

3.5.AD - ACTIVE DIRECTORY – umożliwia zarządzanie tożsamościami i relacjami tworzącymi sieć organizacji. Zawiera informacje m. in. o serwerach, komputerach, użytkownikach, grupach i wszelkich innych obiektach występujących w sieci organizacji.

4. **WYZWALACZE**

Zdarzenia inicjujące proces zarządzania uprawnieniami dostępu:

4.1.Zmiany kadrowe:

1) nawiązanie stosunku pracy,

2) rozwiązanie stosunku pracy,

3) zmiana warunków umowy o pracę w zakresie zmiany stanowiska pracy, jednostki Urzędu.

4.2.Zmiana zakresu czynności.

5. DANE WEJŚCIOWE PROCESU

1) polityka bezpieczeństwa,

2) wymaganie dotyczące uprawnień dostępu, potrzebne do podejmowania działań administracyjnych w zakresie zarządzania uprawnieniami dostępu oraz do efektywnego odpowiadania na wydarzenia powiązane z uprawnieniami dostępu,

3) dane pracownika, którego dotyczy działanie związane z zarządzaniem uprawnieniami,

4) informacja o czynności, którą należy wykonać (nadanie/zmiana/przedłużenie/odebranie),

5) zakres uprawnień dostępu.

6. PRZEBIEG PROCESU

6.1.Proces zarządzania uprawnieniami dostępu odbywa się tylko w formie elektronicznej zgodnie z załącznikiem nr 1 do procedury zarządzania uprawnieniami dostępu do zasobów/systemów informatycznych Urzędu Miasta Szczecin.

6.2.Wniosek, dotyczący uprawnień pracownika w formie elektronicznej, dalej wniosek, przygotowuje pracownik ds. organizacyjno-biurowych jednostki wnioskującej.

Wzór wniosku stanowi załącznik nr 2 do procedury zarządzania uprawnieniami dostępu do zasobów/systemów informatycznych Urzędu Miasta Szczecin.

6.3.Wniosek w zależności od rodzaju zmian kadrowych, zmian zakresu czynności może dotyczyć:

1) **nadania/udzielenia uprawnień**

występuje w przypadku potrzeby przydzielenia nowych uprawnień do zasobów/systemów informatycznych, których do tej pory pracownik nie posiadał,

2) **odebrania/anulowania uprawnień**

występuje w przypadku potrzeby odebrania dostępu do zasobów/systemów informatycznych, które należy wskazać we wniosku,

3) **zmiany uprawnień**

występuje w przypadku potrzeby rozszerzenia lub zmniejszenia przydzielonego dostępu do zasobów/systemów informatycznych,

4) **przedłużenia uprawnień**

występuje w przypadku przedłużenia stosunku pracy bez potrzeby zmiany zakresu, a także poziomu uprawnień.

Wyjaśnienie:

Zmiana kadrowa dotycząca zmiany jednostki przez pracownika Urzędu generuje dwa wnioski:

a) wniosek o odebranie uprawnień, przygotowany przez pracownika ds. organizacyjno-biurowych jednostki, w którym pracownik zakończył pracę,

b) wniosek o nadanie uprawnień, przygotowany przez pracownika ds. organizacyjno-biurowych jednostki, w którym pracownik rozpoczął pracę.

6.4.Wniosek przygotowany przez pracownika ds. organizacyjno-biurowych jednostki wnioskującej powinien być zaakceptowany przez Kierownika.

6.5.Wniosek przekazywany jest bezpośrednio do Wydziału Informatyki Urzędu.

6.6.Wniosek dotyczący nadania, zmiany, przedłużenia uprawnień należy zweryfikować czy dotyczy zasobu/systemu informatycznego, dla którego wymagane jest wyrażenie zgody na przetwarzanie danych przez Właściciela zasobu:

1) jeżeli TAK: wniosek zostaje przekazany do Właściciela zasobu,

2) jeżeli NIE: wniosek jest przekazywany do Wydziału Informatyki Urzędu.

6.7.Właściciel zasobu rozpatruje wniosek i udziela odpowiednio akceptacji. Zgoda na dostęp do systemu/zasobu informatycznego określa poziom uprawnień.

6.8.Właściciel zasobu przekazuje, do jednostki wnioskującej o uprawnienia, informację o udzielonej zgodzie wraz z wnioskiem.

6.9.Pracownik ds. organizacyjno-biurowych jednostki wnioskującej, po otrzymaniu odpowiedzi od Właścicieli zasobu, weryfikuje wniosek, następnie przekazuje go do Wydziału Informatyki Urzędu.

6.10.Wydział Informatyki Urzędu otrzymuje wniosek dla pracownika.

6.11.Wydział Informatyki Urzędu dokonuje weryfikacji wniosku pod względem poprawności:

1) formularza wniosku,

2) osoby wnioskującej,

3) wyrażenia zgód przez Kierownika jednostki wnioskującej oraz Właścicieli zasobu,

4) wypełnienia pozycji obowiązkowych.

6.12.Wynik przeprowadzonej weryfikacji wniosku decyduje o dalszym postępowaniu:

1) jeżeli wniosek jest poprawny zostaje przekazany do realizacji,

2) jeżeli wniosek nie jest poprawny zostaje zwrócony pracownikowi ds. organizacyjno-biurowych jednostki wnioskującej wraz ze wskazaniem jego nieprawidłowości.

6.13.Wydział Informatyki Urzędu rejestruje wniosek w systemie informatycznym.

6.14.Zarejestrowany wniosek jest weryfikowany, analizowany oraz uzupełniany niezbędnymi informacjami przez Wydział Informatyki Urzędu.

6.15.Analiza zarejestrowanego wniosku - czy dotyczy działań związanych z Active Directory:

1) jeżeli TAK: wniosek zostaje przekazany do Administratora Systemu Informatycznego (ASI),

2) jeżeli NIE: następuje punkt 6.16.

6.16.Analiza zarejestrowanego wniosku - czy dotyczy kilku Administratorów Systemu Użytkowego (ASU):

1) jeżeli TAK: wykonywana jest odpowiednia ilości kopii zarejestrowanego wniosku,

2) jeżeli NIE: następuje punkt 6.17.

6.17.Zarejestrowany wniosek przekazany jest do właściwego ASU.

6.18.ASU realizuje zarejestrowany wniosek.

6.19.ASU informuje o realizacji wniosku:

1) bezpośredniego przełożonego pracownika,

2) pracownika ds. organizacyjno-biurowych,

3) pracownika, którego dotyczy uprawnienia,

4) odpowiednio właściciela zasobu.

6.20.Pracownik, którego dotyczył wniosek, weryfikuje poprawność realizacji wniosku.

7. DANE WYJŚCIOWE PROCESU

1) zapewnienie dostępu do usług IT na podstawie polityki bezpieczeństwa informacji,

2) zapis i historia udzielanych uprawnień dostępu,

3) zapis i historia odebranych uprawnień wraz z określeniem przyczyny,

4) komunikacja w zakresie naruszeń dostępu,

5) informacja o statusie realizacji wniosku.

8. ODPOWIEDZIALNOŚĆ I UPRAWNIENIA

Matryca odpowiedzialności stanowi załącznik nr 3 do procedury zarządzania uprawnieniami dostępu do zasobów/systemów informatycznych Urzędu Miasta Szczecin – Matryca odpowiedzialności.

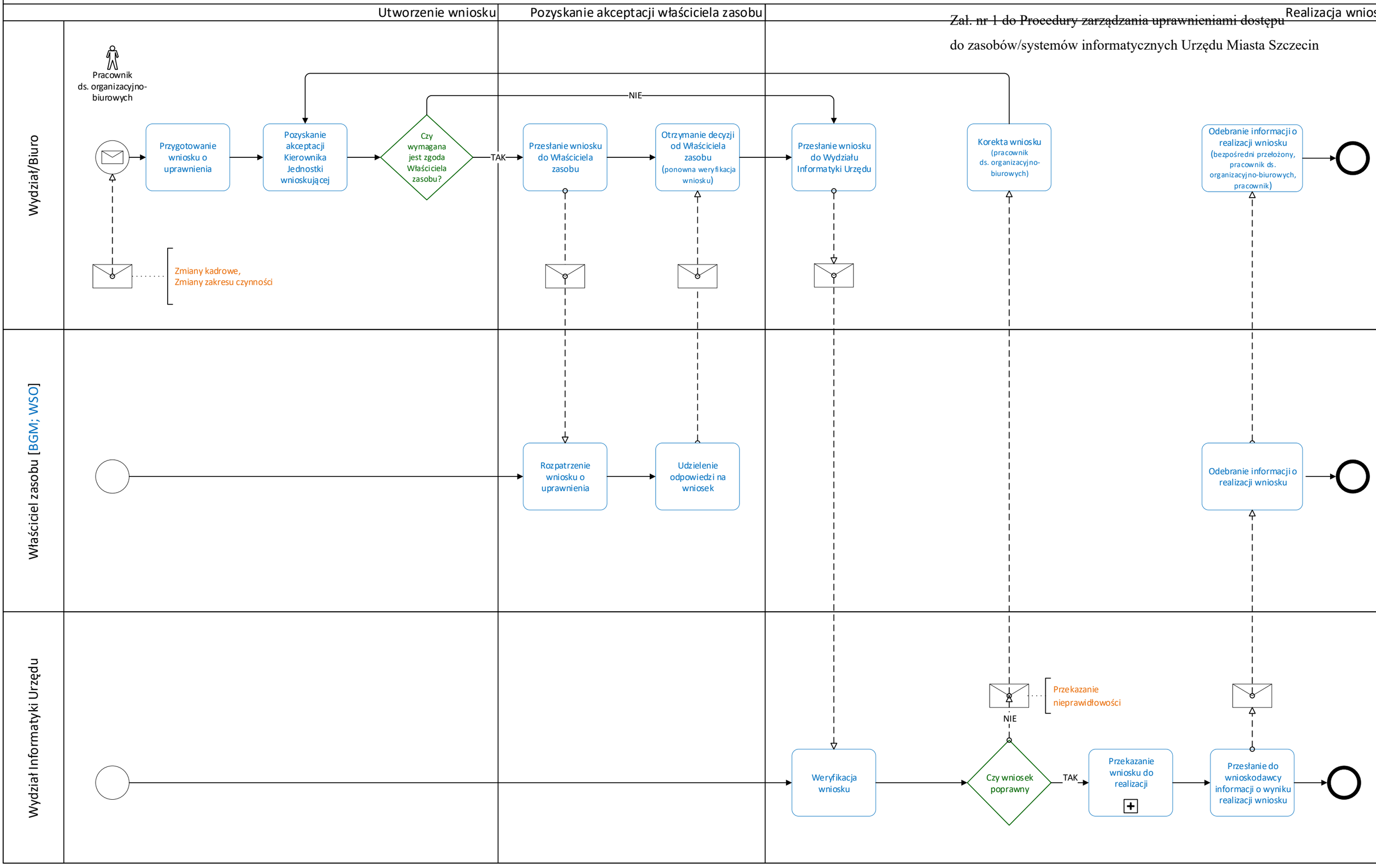
1) **Pracownik ds. organizacyjno-biurowych jednostki wnioskującej** – posiada uprawnienia do przygotowania wniosku dla pracownika oraz do przekazania go do właściwych Jednostek, zgodnie z procesem zarządzania uprawnieniami. Odpowiada za poprawność formalną wniosku.

2) **Kierownik jednostki wnioskującej** – posiada uprawnienia do zatwierdzania wniosku oraz odpowiada merytorycznie za zakres uprawnień dla pracownika nim zawarty.

3) **Właściciel zasobu** – posiada uprawnienia do zatwierdzania wniosku oraz odpowiada merytorycznie za zakres uprawnień dla pracownika dotyczący jego zasobów/systemów informatycznych.

4) **Wydział Informatyki Urzędu** – posiada uprawnienia do realizacji wniosku, odpowiada za wykonanie zadań zgodnie z polityką bezpieczeństwa.

PROCES ZARZĄDZANIA O UPRAWNIENIAMI DOSTĘPU DO ZASOBÓW/SYSTEMÓW INFORMATYCZNYCH URZĘDU MIASTA SZCZECIN



Zał. nr 2 do Procedury zarządzania uprawnieniami dostępu
do zasobów/systemów informatycznych Urzędu Miasta Szczecin

Szczecin, dnia…

WNIOSEK DOTYCZĄCY UPRAWNIEŃ PRACOWNIKA

NADANIE / ZMIANA / PRZEDŁUŻENIE / ODEBRANIE *

Jednostka organizacyjna: .....
Imię i nazwisko: .....
Nr ewidencyjny pracownika: .....
Stanowisko lub rodzaj pracy: .....
Referat: .....
Nr pokoju (stary/nowy): .....
Telefon: .....

Czy osoba była wcześniej pracownikiem UM i miała założone konto w systemie informatycznym*: TAK/NIE
Identyfikator sieciowy (login)**: .....

Oprogramowanie*:

- Rejestr: poziom*: delegatura wydziału; sekretariat wydziału; kierownik referatu; referent; kierownik WSO; kancelaria WSO
- SIP - System Informacji Przestrzennej uzyskać akceptację od BGM
  wybierz poziom*: poziom 1 - podstawowy (imię, nazwisko, KW); poziom 2 - rozszerzony (pełne dane osobowe)
- iEGIB uzyskać akceptację od BGM
- BBD - Ewidencja Ludności PESEL uzyskać akceptację od WSO
  wybierz poziom*: dane personalne; PESEL; rok urodzenia; karta zgonu; płeć; adres czasowy; adres poprzedni; dowód tożsamości; dane z USC; nazwisko rodowe; nazwisko poprzednie; imię matki; nazwisko rodowe matki; płeć, obywatelstwo
- BBD - Wydawanie Poświadczeń
- BBD - Rejestry Wydziału Urbanistyki
- DoKasy
- DoKasy z obsługą terminala
- ICOR SOK => poziom *: nadawca; sekretariat, sortownik, archiwista, zwrotki
- ICOR UM - BIP
- ICOR UM - UMINET - Zarządzenia Prezydenta
- Lex
- Kostka analityczna - budżetowa*, hurtowniana*, strategiczna*
- Środowisko Raportowe (raporty budżetowe, opisowe i inne) - dostępne z przeglądarki
- Q-matic: Lewobrzeże, Prawobrzeże, USC, stanowisko, recepcja, statystyki, podgląd, kalendarz, koordynator, kierownik
- ZSI-FK
- Inne: .....

.....
.....
Rodzaj umowy: .....
Zatrudniona/y od .....do .....
Pracownik posiada upoważnienie do przetwarzania danych osobowych: TAK/NIE
Pracownik posiada dostęp do tajemnicy skarbowej*: TAK/NIE

W przypadku zmiany komórki organizacyjnej: R
Poprzednia komórka organizacyjna (wydział, referat): .....
Pracownik przechodzi ze sprawami / bez spraw*

* właściwe zaznaczyć, ** wypełnić dla TAK

Zał. nr 3 do Procedury zarządzania uprawnieniami dostępu
do zasobów/systemów informatycznych Urzędu Miasta Szczecin

Matryca odpowiedzialności

	Pracownik ds. organizacyjno – biurowych	Bezpośredni przełożony pracownika, którego dot. uprawnienia	Kierownik jednostki wnioskującej	Właściciel zasobu	Wydział Informatyki Urzędu	Pracownik, którego dot. uprawnienia
Przygotowanie wniosku	R	C	A			I
Akceptacja wniosku		C	AR			
Przekazanie wniosku do Właściciela zasobu	R		A			
Wyrażenie zgody na dostęp do zewnętrznego systemu/zasobu inf.				AR		
Przekazanie wniosku do Wydziału Informatyki Urzędu	R		A			
Weryfikacja wniosku	R	C	AR	AR	AR	
Realizacja wniosku					AR	
Informowanie o statusie realizacji	I	I		I	AR	I

R - Osoba odpowiedzialna za wykonanie zadania

A - Osoba nadzorująca, odpowiedzialna za zatwierdzenie zrealizowanych zadań

C- Osoba pełniąca rolę konsultanta

I - Osoba informowana o prowadzonych działaniach, nie ma wpływu na decyzje z nimi związane