Załącznik Nr 16 do Zarządzenia Nr 150/18

Prezydenta Miasta Szczecin

z dnia 6 kwietnia 2018 r.

Procedura administrowania identyfikatorami i hasłami dostępu w Urzędzie Miasta Szczecin

Przydzielanie identyfikatorów i haseł użytkownika odbywa się w sposób zgodny z poniższymi zasadami:

1. Użytkownik systemu informatycznego musi posiadać unikalny identyfikator i hasło.

2. Użytkownik posługuje się jednym identyfikatorem aby uzyskać dostęp do zasobów sieciowych, wszystkich systemów i baz danych.

3. Identyfikator i hasło użytkownika nadaje ASI na pisemny wniosek Kierownika.

4. Identyfikator użytkownika jest w systemie informatycznym Urzędu unikatowy. Z uwagi na dużą liczbę użytkowników systemu informatycznego będących pracownikami Urzędu jak i jednostek podległych, a także instytucji i firm zewnętrznych wykonujących określone zadania zlecone przez Urząd, unikalny identyfikator użytkownika może mieć zróżnicowaną budowę. Najczęściej składa się on z pierwszej litery imienia i całości lub części nazwiska lub z pełnego imienia, kropki i pełnego nazwiska. Dopuszcza się także inną, zbliżoną do ogólnej zasady budowę identyfikatorów w systemie (szczególnie w sytuacjach powtarzających się imion i nazwisk użytkowników). Niezależnie od zdefiniowanego identyfikatora użytkownika systemu informatycznego, jest on powiązany z danymi użytkownika tj. pełnym imieniem i nazwiskiem, komórką organizacyjną w której użytkownik pracuje (na rzecz której wykonuje zlecone przez Urząd zadania) i dzięki tym danym można w pełni zidentyfikować konkretnego użytkownika (szczególnie w sytuacjach zbieżności imienia i nazwiska).

5. Raz przydzielony identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu nie może być przydzielany innej osobie, nawet gdy konto to jest nieaktywne.

6. Dopuszcza się zmianę identyfikatora tylko w szczególnych przypadkach na pisemny wniosek użytkownika w sytuacji gdy osoba go posiadająca zmieniła swoje dane personalne. Fakt ten jest rejestrowany w ewidencji, o której mowa w ust. 9.

7. Identyfikator osoby, która utraciła uprawnienia dostępu do danych należy niezwłocznie zablokować w systemie informatycznym.

8. Osobą odpowiedzialną za powiadomienie ASI i ASU o konieczności wyrejestrowania użytkownika jest Kierownik.

9. Użytkownik systemu informatycznego, w którym przetwarzane są dane osobowe, jest zarejestrowany w ewidencji prowadzonej przez ASI. Ewidencja zawiera następujące informacje:

1) imię i nazwisko,

2) identyfikator,

3) pierwsze hasło,

4) data wpisania do systemu,

5) data wyrejestrowania z systemu.

10. Hasło użytkownika powinno być utrzymywane w tajemnicy zarówno w czasie jego ważności jak i po tym terminie.

11. Hasło użytkownika powinno być zmieniane nie rzadziej niż co 30 dni. Jeżeli system lub baza danych nie wymusza okresowej zmiany hasła to nadzór nad terminową zmianą haseł przez użytkowników prowadzą administratorzy systemów/baz danych.

12. Hasło użytkownika powinno składać się z co najmniej 8 znaków i zawierać kombinację liter i cyfr i znaków specjalnych.