Title	**User IDs**
Type	Standard
Related Policy	User ID Security
Category	Security
Status	Approved
Approved	02/15/2013
To Be Reviewed	06/18/2017
Scope	Applies to all User IDs issued to access City information technology assets.
Standard	1. Password shall consist of at least eight (8) characters, containing three of the four following categories of characters; capital, lower, numbers, special (e.g. ^, $, @ etc…) 2. The prefix character shall be 'E' for City employees, 'W' for Water Utility Authority employees, and 'X' for all other external entities including contactors. 3. The five-digit suffix shall be the employee number for City and Water Utility Authority employees. 4. The five-digit suffix for external users shall be assigned by the DTI Service Desk. 5. Assigned User IDs shall never be reused, but rather disabled and recorded. 6. Existing User IDs will be valid until a new User ID needs to be issued. 7. New "legacy" User IDs with three-character "system ID" can be issued for legacy systems which require IDs compliant with the previous standard. 8. Non-City employees will be identified and will limited to six (6) months access extension of six (6) months can be requested by the managing department. Non-City employees **cannot** request extensions.
Rationale	User ID assignment and re-assignment is a labor intensive operation that often confuses users of City IT assets. By using the employee number in the User Id, the intention is for an employee to have one User ID throughout their career with the City, regardless of the role in which they perform or the current organization structure of City Government. In addition, prohibiting re-use of User Ids can assist the City in complying

with future court-ordered discovery processes.