Title	**User ID Security**
Type	Policy
Category	Security
Status	Approved
Approved	01/09/2013
Revised	06/06/2015
Scope	Applies to all City information technology assets requiring access by User ID. This policy shall not apply to User IDs for the following: • role accounts required for infrastructure support such as system, database, or network administration; • batch processing; • non-interactive environments (e.g., process control, data acquisition) ; • test environments or training labs where no access to production systems is available; • Bernalillo County accounts on the City's systems.
Policy	1. Any transaction performed upon a City information technology asset which alters data (e.g., adds, changes, deletes) or displays data which is not subject to public disclosure shall be performed using a City-issued User ID **which uniquely identifies the individual performing the transaction.** 2. Access to any City information technology asset shall be granted at the discretion of the owner of the asset (e.g., DFAS/Accounting shall determine who shall be granted access to the General Ledger and Payroll systems). Potential users must secure the approval of the owner of information technology asset prior to requesting that the Department of Technology and Innovation (DTI) or a Department grant access to the asset. The owner of the asset may restrict a user's access on a need-to-know, need-to-do basis, notwithstanding the provisions of the New Mexico Inspection of Public Records Act. 3. Unique User IDs of a standard format, with passwords, shall be required to access all multi-user computer systems. The User ID shall be uniform across all system platforms, and shall follow the formatting standard for User IDs. DTI shall maintain a central repository of assigned User IDs, and coordinate with central and departmental System Administrators and the appropriate Human Resources functions.

4. Contractors or employees of non-City agencies who access City applications shall be issued User IDs which identify them as external users of City information technology assets, which shall be generated as defined above.
5. User IDs and passwords shall not be shared among users. Exceptions to the use of shared User IDs may be granted by the DTI Security Officer upon approval of the Technical Review Committee (TRC). A procedure for requesting and granting exceptions shall be published. The excepted systems shall be published in a standard. Exceptions shall be granted only if the DTI Security Officer determines that sufficient controls exist for the system to comply with City policies and regulations concerning the protection of City information technology assets. Budgetary and/or convenience issues alone shall not be considered sufficient justification for exception to this policy. The TRC may, at its discretion, periodically review and recommend modifying or revocation of existing exceptions.
6. A standard shall be published detailing specifications for passwords, including but not limited to minimum length; combination of alphanumeric and non-alphanumeric characters, expiration intervals, initial password assignment, and encryption.
7. A system shall automatically inhibit the use of a User ID after a standard number of access attempts with an incorrect password. The System Administrator or responsible function shall reactivate the User ID only after verifying the identity of the user. System Administrators shall quarterly review user access and suspend any user account that has not been active for a three month period. Any account in a suspend mode for three months shall be removed.
8. A system shall not permit the re-use of prior passwords for a minimum standard number of iterations.
9. A system shall automatically terminate a user session after a minimum standard period of inactivity.
10. A system shall provide an audit trail of transactions performed identifying the user who initiated the transaction, the date and time of the transaction, type of entry, and what data was accessed or altered. This information shall be retained for a minimum standard time period, notwithstanding additional retention periods which may be mandated by other policies or by law.
11. Unsuccessful access attempts and access violations shall be automatically logged, reported, and reviewed by the System Administration or Security Administration function for appropriate follow-up.

Rationale	The City of Albuquerque relies extensively on its computing systems to meet its operational, financial, and informational requirements. It is essential that these systems and the data they process be operated and maintained in a secure environment. The intent of this policy is to maintain accountability. Protection of City assets and accountability for their use shall override convenience in all circumstances.