Department of Technology and Innovation

User Accounts and Security Standard

TITLE:	User Accounts and Security
TYPE:	Standard
RELATED POLICY:	User Accounts and Security Policy
CATEGROY:	Security
EFFECTIVE DATE:	March 2, 2023
REVISED DATE:	March 1, 2023

1. PURPOSE:
   The purpose of this standard is to establish guidelines for the City of Albuquerque (COA) to uniquely identify each technology asset user.

2. SCOPE:
   Applies to all City information technology assets as noted under the User Accounts and Security Policy.

3. STANDARD:
   a. 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 regularly (quarterly is highly recommended, annually is the minimum requirement) 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 permanently suspended. When an individual leaves the City, his or her account(s) must be locked as soon as reasonably possible and, subsequently, deleted within a reasonable time. If misuse or theft is detected or suspected, account(s) will be locked according to the City's procedures.
   b. A system shall not permit the re-use of prior passwords for a minimum standard number of iterations.
   c. A system shall automatically terminate a user session after a minimum standard period of inactivity.
   d. A system should 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.
   e. Users are responsible for keeping accounts and passwords confidential and for safeguarding City data and information, regardless if it is stored on City computing resources, stored on non-City resources, or being transmitted over communication networks.

f. Users shall not supply their City credentials (e.g. email address) for personal use, software, and/or services.

4. ENFORCEMENT:
   Violation of this policy shall be reported to the appropriate supervisor and may be subject to potential disciplinary action, up to and including termination.

5. EXCEPTIONS:
   Limited exceptions to the standard may be granted by the Director of the Department of Technology and Innovation on a case-by-case basis.

6. RESOURCES:
   Resources may be modified by TRC. Standards will be developed in accordance with the resources below. The city shall endeavor to maintain compliance with the following resources: