Department of Technology and Innovation

Password Standard

TITLE:	Password Standard
TYPE:	Standard
RELATED POLICY:	User Accounts and Security Policy
CATEGROY:	General
EFFECTIVE DATE:	Jan. 9, 2013
REVISED DATE:	June 22, 2022

1. SCOPE:
   Applies to user accounts on all City systems capable of setting user password complexity. For purposes of this standard, the Director of the Department of Technology and Innovation (DTI) is considered to be the Chief Information Officer. Information Security Officer (ISO) refers to the City's top Cybersecurity authority as designated by the Director of DTI.

2. RATIONALE:
   The City of Albuquerque's network and information systems provide the technical foundation for the conduct of its operational and administrative missions. These systems and the data they process are operated and maintained in a secure environment. Account holders are held responsible for all activities associated with their accounts, and thus the strength and protection of passwords is critical to ensuring that unauthorized activity does not become associated with an account. This standard is to establish the **minimum** requirements for acceptable passwords and the processing requirements for information systems managing them.

3. STANDARD:
   The Director of Department of Technology and Innovation or designee is hereby authorized to mandate more stringent standards should security conditions require such. The more stringent standards shall be brought before the TRC at the next regularly held meeting.

A. Non-Administrator and Non-Service Account

- Passwords shall contain at least 14 characters including a number, an upper-case letter, and a special character. Exceptions may be authorized by the Chief Information Officer (or designee).
- Each individual user will have their own password(s), which shall never be shared.

- Passwords will be extant no more than 90 days (current practice for users is 84 days). Exceptions may be approved by the Chief Information Officer (or designee).
- Multiple sign-on authority (also known as shared accounts) must be authorized by the user's department manager and approved by the Chief Information Officer (or designee).
- Passwords shall not be reused for 10 cycles or one year.
- When possible, Active Directory is to be used for system authentication.
- DTI reserves the right to maintain the integrity of passwords by creating a password ban list.

B. **Administrator Account**

- Passwords shall contain at least 20 characters including a number, an upper-case letter, and a special character. Exceptions may be authorized by the Chief Information Officer (or designee).
- Passwords will be extant no more than 90 days (current practice for users is 84 days). Exceptions may be approved by the Chief Information Officer (or designee).
- Multiple sign-on authority (also known as shared accounts) must be authorized by the user's department manager and approved by the Chief Information Officer (or designee).
- System supervisor, super user, and administrator passwords must be recorded in a secure location accessible to the ISO and Chief Information Officer (or designee).
- Passwords shall not be reused.
- When possible, Active Directory is to be used for system authentication.
- DTI reserves the right to maintain the integrity of passwords by creating a password ban list.

C. **Service Account**

- Passwords shall contain at least 20 characters including a number, an upper-case letter, and a special character. Exceptions may be authorized by the Chief Information Officer (or designee).
- Passwords will be extant no more than 90 days (current practice for users is 84 days). Exceptions may be approved by the Chief Information Officer (or designee).

- Multiple sign-on authority (also known as shared accounts) must be authorized by the user's department manager and approved by the Chief Information Officer (or designee).
- Service Account passwords must be inventoried and recorded in a secure location accessible to the ISO and Chief Information Officer (or designee).
- Passwords shall not be reused.
- When possible, Active Directory is to be used for system authentication.
- DTI reserves the right to maintain the integrity of passwords by creating a password ban list.

4. EXCEPTIONS:
   Limited exceptions to the standard may be granted by the Director of the Department of Technology and Innovation (or designee) on a case-by-case basis.

5. RESOURCES:
   Resources may be modified by TRC. The city shall endeavor to maintain compliance with the following resources:
   - Awareness training for password creation