PASSWORD STANDARD

ORIGINATION DATE:	**01/09/2013**
EFFECTIVE DATE:	**01/09/2013**
VERSION:	**2.0**
ISSUED BY:	**DTI CYBERSECURITY**
APPROVED BY:	**TRC**
DATE APPROVED:	**10/26/2021 (REVISED)**

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 is considered to be the Chief Information Officer.

- Passwords shall contain at least 8 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 should 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 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 for three cycles or one year
- When possible, Active Directory is to be used for system authentication.

DTI Security reserves the right to maintain the integrity of passwords by creating a password ban list. Password Banning is the system enforced check on new password creation against an internal deny list of known bad, weak, or recently used passwords.

Rationale: The City of Albuquerque's network and information systems provide the technical foundation for the conduct of its operational and administrative missions. It is essential that these systems and the data they process be 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. The intent of this standard is to establish the minimum requirements for acceptable passwords and the processing requirements for information systems managing them.

References:

Awareness training for password creation