Title	**Passwords Standard**
Type	Standard
Related Policy	User ID Security
Category	Security
Status	Approved
Approved	01/09/2013
Revised	06/16/2015
Scope	Applies to user accounts on all City systems capable of setting user password complexity. This replaces the "Novell NetWare Login Passwords" standard.
Standard	Policy Provisions: • Passwords shall contain at least eight characters including a number or special character • Each individual user will have their own password(s), which should never be shared with another person • Passwords will be changed every 90 days; automated notification will be sent out to staff five days prior to password expiration • Passwords for critical resources e.g. server Administrative passwords, must be changed on a 90 cycle or if suspicious activity is suspected • The user sign-on will (on systems supporting this function) be disabled for at least 15 minutes after five (5) unsuccessful login attempts • multiple sign-on authority must be authorized by the user's department manager • System supervisor, super user, and administrator passwords must be recorded in writing, sealed in a labeled envelope, and deposited in a locked receptacle in either the agency head’s office or a vault. Keys to the receptacle will be kept by the ISO and Chief Information Officer. In case of an emergency, the envelopes can be accessed, after which the password(s) are changed and resealed; • Temporary employees will have passwords set by DTI and the individual staff supervisor. Accounts will expire at the end of the temp's contracted time. Supervisors must authorize renewal of such user accounts when they expire • Passwords shall not be reused for three cycles or one year • When possible, Active Directory is to be used for system authentication. • It is recommended that passwords should not contain words that

	can easily be guessed like “password”, your child’s name, your dog’s name, etc. and should not be written down in an accessible location..
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.