City of Phoenix

Information Technology Standard

Domain:	Number:	Standard Title:
Information Security	s1.5	Password Management

Original Approval	11/20/2009	**Last Updated/Approved**	09/20/2010
Compliance Date	5/20/2011	**Last Reviewed**	08/16/2010
Owner	ISPO/PMO		
Approvals	IT Governance Operational Committee		

I. Purpose – Summary of Intent

This standard establishes acceptable practices for creating and maintaining passwords.

II. Definitions – Terms Specific to the Standard

- **City Personnel** – Anyone authorized to access City information systems and information including, without limitation, City of Phoenix employees, business partners, contractors, volunteers, and temporary workers.

- **Privileged Account** – a computer account or access that has administrative, root, or super user privileges.

III. Applicability

This standard applies to City personnel who have access to City information and computer systems. This standard applies to passwords for all City of Phoenix Information Systems. This standard supersedes the previous version of this standard, s1.5 Password Creation and Maintenance. City personnel must comply with this standard no later than 18 months after this standard is approved.

IV. Standard

1.0 Password Requirements

1.1 Password Characteristics. Passwords must meet these requirements:

- Passwords must be at least 8 characters for all accounts.

- Passwords must contain a combination of at least three of the following:

    - Uppercase character (A-Z)
    - Lowercase character (a-z)
    - Number (0-9)
    - Special character (e.g. !, @, #). Do not use ?, %, or *.

- Passwords must not be:
    - Individual-related (e.g. address, birthday, license plate, social security number, pet's name)
    - Job-related (e.g. job title, work location)
    - Family-related (e.g. spouse's or children's names or birthdays)
    - Similar to or match the User ID
    - Dictionary words, or
    - Predictable (e.g. X34s!JAN, X34s!FEB, X34s!MAR).

- To remember passwords easily, personnel are encouraged to use passphrases. Example: take the first letter from every word in a line from a song:
    - Jingle bells, jingle all the way: Jbjatw2@
    - Just like the white winged dove: Jltwwd1!

1.2 Password Change Frequency

- Passwords must be changed at least every 60 days.

- If the system supports forcing password changes, the system must force the password to change at least every 60 days.

1.3 Password Privacy

- Passwords must be encrypted in non-volatile storage and in transit.

- Passwords must never be shared with any user for any reason.

- City personnel should only write passwords down if they can't remember them. If City personnel elect to write their passwords down, they must store the password in hardcopy format in a locked location, and they must be the only person who has access to the locked location.

- Passwords must be masked or hidden upon logging into the system so they cannot be seen in clear text.

- Passwords must not be stored as clear text in scripts, programs, or files.

1.4 No Password Reuse on the Same System

- Passwords must not be reused or be similar to previous passwords.

- Systems that can track history of passwords used in an encrypted format must prohibit password reuse. These systems must track password history for at least the last 12 password changes.

1.5 Compromised Passwords. City personnel must report compromised, lost, or stolen passwords to department technical contacts immediately. Department technical contacts must reset the compromised password immediately.

1.6 Privileged Account Passwords. City personnel with a privileged account must have a different password from all other accounts.

2.0 Password Administration

2.1 New and Reset Passwords

- Administrators must provide new or reset passwords to City Personnel verbally after verifying the individual's identity. Administrators must never write passwords down or send them over unencrypted email. Departments that perform password resets over the phone must maintain and follow an SOP to verify the user's identity.
- New or reset passwords must be unique for each user.
- After City personnel use the new or reset password to login, they must change their password.
- If the system supports forcing password changes after initial login, the system must force the user to change their password.
- Self-service password resets require a minimum of three security questions to verify identity.

2.2 Change Default Passwords. Prior to deployment, default passwords must be changed.

V. Compliance Audits

The City Auditor Department may conduct periodic audits to evaluate compliance with the requirements set forth in this IT standard.

City personnel must comply with this standard at all times. City of Phoenix reserves the right to monitor systems, electronic communications, and usage to ensure compliance.

VI. Related Policies , Standards, and Procedures

A.R. 1.63, Electronic Communications and Information Acceptable Use

A.R. 1.84, Information Security Management

A.R. 1.90, Information Privacy and Protection

A.R. 1.91, Information Privacy and Protection Supplement — Data Shared with Third Parties

A.R. 3.96, Merchant Accounts (Payment Card Processing)

s1.3 Identity Management Standard

b1.3 Waiver Standard