

ATTACHMENT O

PASSWORD MANAGEMENT STANDARD



City of Phoenix Enterprise Information Technology Standard

Domain: Privacy & Compliance			Number: 300-015	Title: Password Management Standard			
Authorizing A.R.(s):			A.R. 1.69 Payment Card Industry Compliance Program				
Authoring Policy:			A.R. 1.84 Information Security Management ISP-300-015 Password Management Policy				
Regulatory Framework:			PCI DSS Requirements Version 3.2.1 NIST Special Publication (SP) 800-53 Revision 5 Criminal Justice Information Services (CJIS) Security Policy Version 5.8				
Original Approval:			9/22/2022				
Number	Version	Pages	Effective Date	Last Review	Next Review	Approved by	Distribution
1	1.0	4	9/22/2022	9/22/2022	9/22/2025	CISO	Online

I. PURPOSE AND APPLICABILITY

The Password Management Standard establishes acceptable practices for creating and maintaining passwords for information systems across the City of Phoenix technology environment, known as the Enterprise.

This standard applies to City personnel who have authorized access to Enterprise information and resources, such as on-prem and cloud-based information systems. For this standard, the “City of Phoenix” is sometimes referred to as the “City”.

II. BACKGROUND

Passwords are the most frequently utilized form of authentication for accessing the City’s Enterprise information systems. Due to the use of weak passwords, the proliferation of automated password-cracking programs, and the activity of malicious hackers and spammers, they are very often the weakest link in securing data. This version replaces *s1.5 Password Management*.

III. DEFINITIONS

For definitions of terms and acronyms, see the [ISG-000-003.1 Information Security Glossary](#). The following terms and/or acronyms are used in this standard:

1. City Personnel
2. Enterprise
3. ISP – Information Security Policy
4. ISPO – Information Security and Privacy Office
5. NIST – National Institute of Security Technology
6. Password
7. PII – Personally Identifiable Information

Domain: Privacy & Compliance	Number: 300-015	Title: Password Management Standard
------------------------------	-----------------	-------------------------------------

IV. STANDARD

Passwords must meet these requirements:

1. Passwords must be at least 14 characters for all accounts.
2. Passwords must contain all 4 of the following elements:
 - 2.1. Uppercase character (A-Z)
 - 2.2. Lowercase character (a-z)
 - 2.3. Number (0-9)
 - 2.4. Special character (for example - !, @, #)
3. Passwords must not be:
 - 3.1. Individual-related (e.g., address, birthday, license plate, social security number, pet's name)
 - 3.2. Job-related (e.g., job title, work location)
 - 3.3. Family-related (e.g., spouse's or children's names or birthdays)
 - 3.4. Similar to or match the User ID
 - 3.5. Dictionary words
 - 3.6. Predictable (e.g., 2023JAN, 2023FEB, 2023MAR)
 - 3.7. Enter content
4. Personnel are encouraged to use passphrases. For example, take the first letter from every word in a line from a song:
 - 4.1 Wlw7,mshmsrfm. = When I was seven, my sister hid my stuffed rabbit from me.
5. Password Change Frequency
 - 5.1. Passwords must be changed at least every 90 days for all Enterprise information systems.
6. Unsuccessful Logon Attempts
 - 6.1. After a maximum of five (5) unsuccessful logon attempts, the system must force an automatic session termination and suspend the User ID for a minimum of 30 minutes or until re-activated by a system or security administrator after verifying the user's identity.
7. Password Privacy
 - 7.1. Passwords must be encrypted in non-volatile storage and in transit.
 - 7.2. Passwords must never be shared with any user for any reason.
 - 7.3. City personnel should avoid writing down their passwords. City personnel are encouraged to use a password vault such as 1 Password, Keeper, Bitwarden, or a similar service. If passwords are written down, they shall be stored in a locked location and be accessible only to the user.
 - 7.4. Passwords must be masked or hidden upon logging into the system so they cannot be seen in clear text.
 - 7.5. Passwords must not be stored as clear text in scripts, programs, or files.
8. No Password Reuse on the same System

Domain: Privacy & Compliance	Number: 300-015	Title: Password Management Standard
------------------------------	-----------------	-------------------------------------

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

8.2. Systems that can track the 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.

9. Compromised Passwords

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

10. Privileged Account Passwords

10.1. City personnel with a privileged account must use a different password than that used for their standard user account if they are not using the City's Privileged Access Management (PAM) system.

11. Password Administration

11.1. New and Reset Passwords

11.1.1. 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 their SOP to verify the user's identity.

11.1.2. New or reset passwords must be unique for each user.

11.1.3. After City personnel use the new or reset password to login, they must change their password.

11.1.4. If the system supports forcing password changes after initial login, the system must force the user to change their password.

11.1.5. Self-service password resets require a minimum of three security questions to verify identity.

11.2. Change Default Passwords

11.2.1. Prior to deployment, default passwords must be changed.

12. Exceptions to Established Standards

12.1. Documentation

12.1.1. Submit a waiver request per b1.3. IT Waiver Standard to request and obtain an exception, in part or whole, to any standard contained within this document related to password management.

12.2. Exception Approval

12.2.1. Must follow the b1.2.1 ITS Waiver SOP.

13. This standard shall be reviewed every three years.

V. POLICIES, STANDARDS, AND PROCEDURES

Additional policies, IT standards, and procedures are developed to augment this standard, as noted:

A.R. 1.69 Payment Card Industry Compliance Program

Domain: Privacy & Compliance	Number: 300-015	Title: Password Management Standard
------------------------------	-----------------	-------------------------------------

A.R. 1.84 Information Security Management
 ISP-300-015 Password Management Policy
 INF-200-201 Identity Management Standard (*Draft*)
 b1.2.1 ITS Waiver SOP


VI. QUESTIONS

Questions regarding this standard should be directed to the Information Security and Privacy Office by emailing ISPO.Policy@phoenix.gov.

VII. APPROVAL

This standard has been approved by:

Acting Chief Information Security Officer


Mitchell Kohlbecker (Jul 11, 2023 10:36 PDT)

Mitchell Kohlbecker
 Deputy Chief Information Officer

07/11/2023

Date

VIII. REVISION HISTORY

Version	Date	Detail of Changes
		N/A