

ATTACHMENT N

IDENTITY MANAGEMENT



City of Phoenix

ENTERPRISE INFORMATION TECHNOLOGY STANDARD

Domain: <i>Infrastructure Architecture</i>			Number: <i>200.201</i>	Standard Title: <i>Identity Management</i>			
Authorizing A.R.			A.R. 1.63 Electronic Communications and Information Acceptable Use A.R. 1.69 Payment Card Industry Compliance Program A.R. 1.73 Control of Communications Services and Systems A.R. 1.84 Information Security Management				
Regulatory Standards			NIST Special Publication (SP) 800-53 Revision 5				
Original Approval			04/02/2024				
Number	Version	Pages	Effective Date	Last Review	Next Review	Approved by	Distribution
200.201	1.0	5	04/02/2024		04/02/2025	T.Magrini	

I. PURPOSE AND APPLICABILITY

This document establishes the City standard for Enterprise Identity Management. It also establishes that Information Technology Services (ITS) is solely responsible for maintaining and controlling the City's Active Directory, Azure Active Directory, and Active Directory Federated Services systems used for controlling authentication and access to City computer resources, applications, and networks.

This standard applies to all workforce personnel – full and part-time employees, persons of interest (POIs), departments, divisions, agencies, and other related City entities.

II. BACKGROUND

Unique identification is fundamental to managing account-based security in any Information Technology (IT) environment. It is essential for any IT-supported system to be able to link all access to specific entities. This standard addresses how the City will create accounts in such a manner to ensure uniqueness and traceability as well as to ensure that identities are managed through a lifecycle appropriate to the entity.

NIST Special Publication (SP) 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, specifies that organizations should implement Identity Management controls.

III. DEFINITIONS

For definitions of terms and acronyms, see the [INF 000.002 Business Operations Glossary](#) and [ISG-000-_____](#). The following terms and acronyms are used in this Standard:

Domain: <i>INF Architecture</i>	Number: <i>200.201</i>	Standard Title: <i>Identity Management</i>
---	----------------------------------	--

- Active Directory (AD)
- Active Directory Federated Services (ADFS)
- Azure Active Directory (AAD)
- Authentication, Authorization and Accounting (AAA)
- Electronic Identification (EID)
- Information Security Office (ISO)
- Multi-factor Authentication (MFA)
- Organizational Unit (OU)
- Person of Interest (POI)
- Public Key Infrastructure (PKI)
- System Owners
- Virtual Private Network (VPN)

IV. STANDARD

1. System of Record

- 1.1. Microsoft Active Directory (AD) is the City's standard for application authentication and access for enterprise and department-owned applications.
- 1.2. The City's standard for application authentication and access for cloud-hosted applications (i.e., Software as a Service) is Azure Active Directory (AAD) and Active Directory Federated Services (ADFS).
- 1.3. Microsoft Identity Manager is the City's standard for integrating Citywide application platforms (i.e., ECHRIS).
- 1.4. The City standard for Multi-Factor Authentication (MFA) is RSA Authentication Manager and RSA Cloud Authentication Service.

2. Roles and Responsibilities

- 2.1. ITS Management Team
 - 2.1.1. The ITS management team, mainly the Assistant Chief Information Officer (ACIO) of Business Operations and Chief Information Security Officer (CISO), will provide governance, oversight, and approval of proposed design and structural changes to the City's Active Directory infrastructure.
- 2.2. Employees, Vendors, and Contractors are responsible for:
 - 2.2.1. Complying with the City's information technology (IT) policies, standards, procedures, and all applicable Federal and State mandates and laws.
 - 2.2.2. Contacting ITS at itd.idm@phoenix.gov with questions about this standard and associated procedures.
- 2.3. Supervisors and Managers are responsible for:
 - 2.3.1. Ensuring employees and contractors understand City IT policies, standards, and procedures.
 - 2.3.2. Holding employees accountable for following City IT policies, standards, and procedures.
- 2.4. IT Back End Platform Architects are responsible for:
 - 2.4.1. Managing all backend logical controls (e.g., Cloud & Identity Management)
- 2.5. Enterprise Administrators are responsible for:
 - 2.5.1. Implementing AD structure, trusts, and services as approved by ITS.

Domain: <i>INF Architecture</i>	Number: <i>200.201</i>	Standard Title: <i>Identity Management</i>
---	----------------------------------	--

- 2.6. Domain Administrators are responsible for:
 - 2.6.1. Managing all objects in their designated AD domain directory infrastructure – parent domains, child domains, sites, and core domain controllers.
- 2.7. VMware and Windows Admins are responsible for:
 - 2.7.1. VMware vCenter Administration
 - 2.7.2. Departmental Organizational Unit (OU) Administration
- 2.8. Department LAN Administrators are responsible for:
 - 2.8.1. Managing all subordinate objects in a departmental OU. The role is required for departmental admins to effectively manage objects (i.e., user, computer, group identities) within their department.
- 2.9. Information Security Office (ISO) personnel and the City Audit Department are responsible for:
 - 2.9.1. Approving and manage updates to Information Security Policies and Procedures.
 - 2.9.2. Managing compliance with all relevant statutory, regulatory, and contractual requirements.
 - 2.9.3. Performing risk assessments and departmental audits to ensure compliance with information security and privacy Administrative Regulations (A.R.), policies, standards, and procedures.

3. Identification and Authentication

- 3.1. City departments must ensure that employees, contractors, and vendors acting on behalf of the department are uniquely identified and authenticated before they are granted access to the City's information systems.
- 3.2. ITS will ensure that all accounts in the City's AD are unique, maintained, and properly configured to ensure compliance with this standard.
- 3.3. ITS is solely responsible for creating user accounts within AD.
 - 3.3.1. User accounts will not be deleted from AD without ITS approval.

4. Identification and Multi-factor Authentication

- 4.1. All City enterprise and department-owned information systems must implement MFA for user access, including privileged accounts.
- 4.2. The Enterprise Identity Management Team will ensure that departments use the City's MFA solution, RSA SecurID Hybrid Cloud Platform, to integrate with their department application systems.

5. Authentication Management

- 5.1. City departments must ensure all users, administrators, system, and privileged account owners are authenticated on all systems by using at least one of the following methods:
 - 5.1.1. Something you know, such as a password, PIN, or passphrase.
 - 5.1.2. Something you have, such as a token device or smart card.
 - 5.1.3. Something you are, such as biometrics.
- 5.2. All authenticators must have sufficient strength for their intended use.
- 5.3. Individual authenticators, including passwords, tokens, biometrics, Public Key Infrastructure (PKI) certificates, and key cards, must be secured by establishing a secured log-on process to minimize the risk of unauthorized access.
- 5.4. The user's identity must be validated before any transaction with information security implications, including modifying or communicating any authentication credential—for example, performing password reset, provisioning new tokens, or generating new keys.

Domain: <i>INF Architecture</i>	Number: <i>200.201</i>	Standard Title: <i>Identity Management</i>
---	----------------------------------	--

6. Authenticator Management | Password-Based Authentication

- 6.1. City departments must enforce minimum password complexity as defined by the City's [Password Management Standard](#).
- 6.2. First-time passwords and reset passwords/phrases must be:
 - 6.2.1. Set to a unique value for each user.
 - 6.2.2. Changed immediately after the first use.
 - 6.2.3. Not stored in the ticketing system.

7. Authenticator Feedback and Cryptographic Module Authentication

- 7.1. Authentication information from a system display must be obscured during authentication to prevent others from seeing the actual characters (i.e., user password).
- 7.2. All authentication credentials (passwords or passphrases) must be cryptographically protected during transmission and storage.

8. Identification and Authentication

- 8.1. City departments must manage all contractors and ensure they are correctly assigned network access to the appropriate systems using the procedures outlined in the City HR system, ECHRIS.
- 8.2. Access to any City enterprise or department-owned application system requires an Employee Identification (EID) or Person of Interest (POI) number assigned in the City's Human Resource system, ECHRIS. User accounts will be created, and names will be using the individual's EID or POI number and legal name or approved preferred name as recorded in ECHRIS.
- 8.3. Accounts used by vendors to access, support, or maintain systems components via remote access must be:
 - 8.3.1. Enabled only during the time needed.
 - 8.3.2. Disabled when not in use.
 - 8.3.3. Monitored when in use.
 - 8.3.4. Accessed only via a City-approved Virtual Private Network (VPN) using MFA.
- 8.4. Group Accounts. Group, shared, or generic IDs, passwords, or other authentication methods must be restricted as follows:
 - 8.4.1. Generic user IDs must be disabled or removed.
 - 8.4.2. Shared user IDs must not exist for system administration and other critical functions.
 - 8.4.3. Shared and generic user IDs must not be used to administer system components.
 - 8.4.4. Passwords and other credentials for group/role accounts must be managed in the enterprise-privileged account management solution to ensure passwords are changed.

9. Re-Authentication

- 9.1. City departments must require users to re-authenticate to access City information systems in the following circumstances or as determined by ITS.
 - 9.1.1. System lock
 - 9.1.2. Role change
 - 9.1.3. After system upgrade/update
 - 9.1.4. To execute privileged functions
 - 9.1.5. To access sensitive data

10. Account Auditing

- 10.1. Quarterly Review
 - 10.1.1. Accounts must be suspended after 90 days of non-use.

Domain: <i>INF Architecture</i>	Number: <i>200.201</i>	Standard Title: <i>Identity Management</i>
---	----------------------------------	--

10.1.2. Where applicable, the account owner's supervisor and the application owner must approve re-activating a suspended account.

10.2. Annual Review

10.2.1. System owners must conduct annual recertifications of all access privileges.

10.2.2. ISSOP-300-013 Enterprise Account Management SOP shall submit the certification.

11. Exceptions to Established Standards

11.1. Submit a waiver request per b1.3.1, ITS Waiver SOP, to request and obtain an exception, in part or whole, to any standard in this document.

V. RELATED POLICIES, STANDARDS, AND PROCEDURES

[A.R. 1.61, Records Management Program](#)

[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](#)

[ISS-300-013 Enterprise Account Security Management Policy](#)

[ISS-300-013.1 Enterprise Account Security Standard – Auditing Standard](#)

[ISS-300-013.2 Enterprise Account Security Management – Provisioning Standard](#)

[ISS-300-015 Password Management Standard](#)

VI. QUESTIONS

Questions regarding this standard should be directed to the ITS ACIO of Business Operations.

This Standard has been approved.

By: Assistant Chief Information Officer, Business Operations


Tom Magrini

April 2, 2024

Date

VII. REVISION HISTORY

Version	Date	Detail of Changes
1.0	04/02/2024	Initial Published version.