City of Phoenix

Information Technology Standard

Domain:	Number:	Standard Title:	
Information Security	s1.3	Identity Management	
* RESTRICTED CITY INFORMATION *			
Original Approval	08/21/2009	**Last Updated/Approved**	09/17/2010
Compliance Date	08/21/2009	**Last Reviewed**	08/16/2010
Owner	ISPO/PMO		
Approvals	IT Governance Operational Committee		

I Purpose – Summary of Intent

The purpose of this standard is to define the minimum key elements related to granting authenticated access to City information and information systems to prevent unauthorized or excessive access.

This standard replaces

- nt1.12 revised, Technology User Identification, and
- s1.3, User-ID Maintenance.

II Definitions – Terms Specific to the Standard

- Administrative account — a type of special function account used to perform system administrative functions. Administrative accounts are often privileged accounts.
- Authentication — the process of determining whether someone or something is, in fact, who or what it is declared to be. For example, knowing the User ID's password is assumed to guarantee that the user is authentic.
- Department Technology Security Liaisons — the City employee that serves as a liaison between ITS and their department to help assure the security and integrity of their department's information and systems.
- Generic account — another term for special function account.
- Identification — the process of identifying an entity, where an entity is a person, device, or process. For example, computer users are identified by their User ID.
- Privileged access — the ability to circumvent the controls of an application or system.
- Privileged accounts — those computer accounts or accesses that have administrative, root, or super user privileges.
- Resource/data owner — the City employee that has approved management responsibility for controlling production, development, maintenance, use, and security of specific assets. Owner does not infer that a person has any property rights to an asset.

- Role-based access control — a method of regulating access to computer or network resources based on the roles of individual users within an enterprise. Roles are often defined based on job, authority, and responsibility within the enterprise.
- Service account — a type of special function account used for machine-to-machine communication, utility programs, and operating system processes. As a general rule, people do not use service accounts, machines do.
- Special function account — a generic term for administrative, service, test, and training accounts.
- Strong authentication — two-factor authentication is considered "strong" authentication, where a factor is
    - Something you know, such as a password
    - Something you have, such as a software- or hardware-based token, or
    - Something you are, such as a fingerprint.
- Test account — a type of special function account used to test systems or applications. Test accounts are not permitted on production systems.
- Training account — a type of special function account used solely for training personnel.

III Applicability

This standard applies to authorized City personnel who manage and authorize access to City information systems and information.

Departmental LAN Administrators are responsible for creating and maintaining unique special function accounts for their departments. The Information Technology Services Department is responsible for issuing special function accounts for enterprise systems covered within the scope of this standard.

The Information Security & Privacy Office has oversight authority for how security and passwords are managed in privileged accounts on enterprise information systems.

IV Standard

1.0 Provisioning

1.1 User IDs. Authorized personnel must establish unique user identifications (User IDs) for each individual user. Authorized personnel must establish unique user identifications (User IDs) for special function accounts, such as time-scheduled jobs or a User ID used to run an application. The User ID must be unique within its own system domain and all other domains in which it is used. Each User ID must have one accountable owner. Each User ID for a non-employee also must have one City employee responsible for the account. If an employee returns to City employment as a non-employee, such as a contractor, he may not use his previous User ID; the non-employee must have a new User ID.

1.2 Requests. All approved requests for access to City information systems and information must be documented and retained per the City records retention schedules.

1.3 Least Privilege. User authorization should be based on the least privilege required to perform assigned tasks.

1.4 Role-Based Access. User authorization may be based on the user's role within the City.

1.5 Account Types and Usage. Listed below are the types of computer accounts used by the City.

This type of account…	Is used for…
User — employee	Individual City employee, including those with non-continuous employment such as seasonal, election, or reserve officer status. New user accounts for employees include network access, access to the City personnel system, and some department-specific access.
User — non-employee	Individual City contractor, consultant, or other non-employee authorized to use City computers and information. New user accounts for non-employees include network access and some department-specific access.
Special function — production	Administrative and service accounts on production systems. These accounts may have privileged access that allows the account owner the ability to circumvent the controls of an application or system.
Special function — non-production	Administrative, service, and test accounts on non-production systems. These accounts may have privileged access that allows the account owner the ability to circumvent the controls of an application or system.
Special function — training	Training accounts on production or non-production systems. These accounts are managed by each department, must follow current passwords in IT Standard s1.5, and should be used only in a controlled, closed environment. Access should be limited to only those applications and services that are required for training.

1.6 Approvals. All requests for access to City information systems and information must be approved by the appropriate approval authorities. Listed below are the minimum required approvals.

This type of account…	Must be approved by the…
User — employee	Requester's supervisor and the resource and/or data owner.
User — non-employee	Requester's supervisor and the resource and/or data owner.
Special function, including training — production	Requester's supervisor and the resource and/or data owner.
Special function, including training — non-production	Requester's supervisor and the resource and/or data owner.

1.7 Account Formats. Listed below are the formatting standards for the types of computer accounts created and used by the City. This does not apply to vendor-supplied special function accounts, such as root or cron.

This type of account…	Has this format…	Where…
User — employee User — non-employee	*nnnnnn*	*nnnnnn* = a 6-digit number containing the individual's City employee ID as defined in the PeopleSoft CHRIS application. Note: Approval to use CHRIS as the authoritative source for non-employees is currently pending.

Special function — production	*DDDRxxxxxxx*	• *DDD* = the department abbreviation
		• *R* = a one-letter designation for the account's role where
		  ○ A = administrator
		  ○ S = service
		• *xxxxxxx* = a 7-digit alphanumeric field that may be contain a unique number or a description of the account's purpose

Special function — non-production	*DDDRxxxxxxx*	• *DDD* = the department abbreviation
		• *R* = a one-letter designation for the account's role where
		  ○ A = administrator
		  ○ S = service
		  ○ T = test
		• *xxxxxxx* = a 7-digit alphanumeric field that may be contain a unique number or a description of the account's purpose

This type of account…	Has this format…	Where…
Special function — training	*TRNxxxxx*	• TRN = recommended training account indicator • xxxxx = recommended alphanumeric field that may contain a unique number or a description of the account's purpose Note: These are suggested formats; training accounts do not have a required format.

1.8 Default Accounts. Authorized personnel must eliminate or disable default system user accounts where technically feasible. If the accounts are required, authorized personnel must document and explain the accounts' use. Immediately after system installation, authorized personnel must change default system passwords.

1.9 Disabling Accounts. Authorized personnel or processes must disable all User IDs, except for the eChris application, for terminated personnel upon notification of termination. As terminated personnel may need to access their personal HR data, an employee's eChris account may remain active for up to 24 months after termination.

Where it is not technically feasible to disable an account, such as for some privileged accounts, authorized personnel must immediately change the account's authenticating information, such as its password, after an individual who had access to the privileged account terminates.

1.10 Suspending Accounts. Where possible, authorized personnel or processes must suspend User IDs after 90 days of non-use. The account owner's supervisor and the resource/data owner, where applicable, must approve re-activating a suspended account.

1.11 Reviewing Accounts. Appropriate supervisors and/or resource/data owners must review access privileges at least annually of all

- Non-employees
- Computer users who have access to personally identifiable or restricted city information, and
- Computer users who have privileged access.

For systems that contain personally identifying, payment card, or Restricted City information, access must be reviewed every 90 days.

2.0 Use

2.1 Authenticating Accounts. Systems must authenticate each user's identity in a manner consistent with the system's protection requirements. Users remotely accessing systems containing personally identifying or Restricted City information must use strong authentication when gaining access to either the City's network or to the specific system.

2.2 Unsuccessful Logon Attempts. 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. For systems containing personally identifying or restricted City information, the system must force an automatic session termination after a three (3) unsuccessful logon attempts.

2.3 Using Privileged Accounts. Those authorized personnel with privileged access must only use that access to perform tasks that require elevated privileges — not for "everyday" tasks. Those authorized personnel with privileged access should aways login with their personal account and use a command such as "su" to switch to a privileged account where technically feasible.

2.4 Remote Vendor Maintenance Accounts. Responsible personnel must enable special function accounts used by vendors for remote maintenance only for the time period needed to perform the maintenance.

Compliance Audits

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

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
A.R. 3.96, Merchant Accounts (Payment Card Processing)
nt1.5, Enterprise eDirectory Design, Administration and Management
b1.3, IT Waiver Standard