IT Security
Agency Policies and Procedures

Access Control Security

Policy Objectives:

The purpose of this document is to document the characteristics of effective access controls and outlines three key principles:

1. Access to information is based upon the employees need to know information to perform his or her duties.
2. Access is provisioned to just the information the employee needs and not more.
3. All employee access is reviewed periodically to validate that the employee has the correct access and that users whose roles have changed have had an appropriate change in information access.

Background Information:

Access control involves the appropriate authorization for access to information and information systems, the proper provisioning of accounts and rights for that account to access information required for users to do their job and reviewing that access to ensure that access is still appropriate. Department of Administration's Access Control Policy outlines the minimum information security requirements for Access Control and the technical controls that enforce best practices. User access to all information and information systems must be approved, provisioned and reviewed.

Scope:

This standard is applicable to all Department of Administration employees, and contractors using Admin computing resources and information. Failure to comply with this policy could result in disciplinary action, up to and including termination of employment.

Responsibilities:

Employees must:

- Follow Access Control procedures.
- Report violations of standards to the Chief Information Officer and their direct supervisor.

Managers must:

- Familiarize themselves with all IT Security Policies.
- Read, understand, and support the IT Security Policies that pertain to their groups function.
- Ensure employees read all applicable IT Security Policies, Standards and procedures required to perform their duties.
- Understand who has a legal or statutory requirement to access information under their control.

Chief Information Officer must:

- Support the technology that enables Access Control.

- Create operational excellence surrounding best practices.
- Monitor Access Control systems and report on threshold exceptions.

Requirements:

General

- Control the addition, deletion, and modification of accounts, credentials, and other identifier objects. Enterprise-wide authentication must be managed through OET's or Department of Administration's Active Directory structure.
- Native operating system authentication can be used to assist enterprise authentication as long as the local operating system performs a proper handoff to an approved Department of Administration or OET Directory Service.
- Require management approval prior to provisioning user access to any IT resource(s).
- Access approval and access provisioning should not be performed by the same person.
- Assign all users a unique ID per security directory.
- Restrict all access based on need-to-know and least privilege.
- If possible, and if necessary enable third party vendor accounts only for the time required to perform necessary business functions.
- Users are assigned default groups based on the Department of Administration department in which they are located. Each default group includes a minimal set of accesses, beginning with basic domain user access.
- All access requests must be approved by the user's manager. Request for access to Department of Administration information that is not public may require additional approval.
- Periodically review access to all computing systems. Revoke inactive accounts in accordance with business systems risk. Identity Management Systems (Active Directory) must disable interactive accounts that are inactive for 30 days (unless prior arrangements have been made) and will delete accounts that are inactive for 90 days (unless prior arrangements have been made).
- Revoke access for terminated users in a timely manner.
- Department of Administration involuntary terminations require immediate removal from Identity Management Systems and will be initiated by manual notification from HR representatives. Voluntary and normal terminations must be processed in a timely manner by the supervisor.
- Review and revoke access for transferred users in a timely manner based upon risk. High risk systems require changes to be made within 15 days.
- Restrict the use of non-user accounts to those situations where there is appropriate authorization. (Required by the operating system or platform).
- Shared User ID's for system administration or Generic user ID's may not be used on systems that contain not public data.
- Access to systems must be identified to a person. The use of individual login's that grant administrative access is encouraged. The use of generic administrative accounts, such as administrator, is discouraged.
- Maintain a record of new, modified, and revoked accounts.
- Maintain a record of access approvals.

Requirements (continued):

Passwords

- Passwords must be unique and known only to the user it is assigned to. Password sharing of any type is prohibited.
- Passwords must be changed upon first login by the new user
- Passwords must adhere to the following requirements:
  - Length of 6 or more characters
  - Contains at least one letter and one number
  - Expire at least every 90 days
  - Cannot be reused for at least 15 changes
  - Locks account after 10 attempts
  - Requires administrative support to unlock account
  - Recommended inactivity screen lockout at 15 minutes

- Password resets or unlocking of accounts performed by IT personnel must positively validate the user's identity prior to reactivating the account.

Security Awareness

- The CIO shall ensure that Agency staff are reminded periodically of the importance of IT security, and are also notified of urgent IT security issues.

Privileged Access

- Restrict privileged access to the least privileged level based on business need-to-use.
- Maintain a record of accounts with privileged access for a minimum of one year.
- Periodically review accounts with privileged access to ensure access is appropriate.
- Require identification, authentication, and authorization to access system utilities.
- Limit the access to system utilities to a minimum number of authorized users.
- Where segregation of duties is required, prohibit access to system utilities for users who have application access.

Session Time-Out

- Require a session time-out after a maximum of fifteen minutes of inactivity
- Require the session time-out mechanism to clear the screen

Application Access Control

- Information Access Restrictions
  - Document any application access restrictions.
  - Restrict application access based on business need-to-use.
  - Restrict access to application system utilities.
  - Restrict an application's access to other applications based on business need-to-use.

Network Access Control and Remote Access

- Access to all networks, wireless networks, and remote access must be authorized, based upon a business need to know and the principle of least privilege.
- Remote access to networks must be approved and use only Department of Administration approved technologies.

Mobile Computing and Communications Access

- Prevent the use of unauthorized, non-Department of Administration approved data phones and PDA devices to connect to the network.
- Require authentication to Department of Administration data systems when using mobile computing devices.
- Require users to protect mobile computing devices to prevent unauthorized access.

Glossary:

User account
A user account consists of a login ID and a password and an associated set of rights to access IT systems and information.

Business Need to Know
Access to information based upon a requirement to perform the designated duties of your job.

Directory
A database of information about users, groups, user information and email accounts associated with User ID's. Systems such as Active Directory from Microsoft, contains a database of users, ID's and associated passwords, and access rights to computer systems and data.

User ID
A user's identification (ID) is the name associated with a person's log-in such as jsmith.

Least privilege
Access to IT systems and information that provides the minimal level of information required to perform you job functions.

Privileged access
Access that has the capability to manage user permissions, manage within or without application restrictions, and monitor system performance or communications.

Provisioning access
The act of setting up a user's account ID, default password and rights to information and information systems.