# Account and Identity Management Policy

## Overview

Information security requires the participation and support of all users with access to [LEP] systems and information. It is the responsibility of every employee, consultant, temporary employee, and contractor of [LEP] (collectively known as “Users”) to help ensure that all information and data are kept secure and available. Likewise, well defined management practices and supports are necessary. Account identification and authentication procedures are one of the key components in this policy.

## Purpose

Computerized user accounts are the means used to grant access to systems and applications. These accounts provide a means of providing standards, security, and accountability across the application pool and system environment for organizational roles. Creating, controlling, and monitoring computer accounts are actions that are critically important to overall security policy and strategy. The purpose of this policy is to provide mechanisms that define and manage accounts for User communities accessing [LEP] resources.

## Scope

This policy applies to all [LEP] Users and management responsible for application identity and role definition within their departments.

## Policy

### GENERAL

Applications and systems in the scope of this policy include but are not limited to operating systems, applications software, tablets, telecommunications equipment, and/or devices or network software that access [LEP] resources.

### ROLES AND RESPONSIBILITIES

**[Information Security Officer (“ISO”)]** – The [ISO] or their designee shall ensure that [LEP] systems and application are protected from unauthorized access by establishing requirements for the authorization and management of user accounts, providing user authentication, and implementing access controls on [Insert Appropriate Department].

**Data Owners/Department Manager** – The data owner for each information system shall be responsible for ensuring that User access requests, authorization and account management are followed for their specific application, User roles are defined, and that appropriate people are assigned the responsibility of overseeing application usage. The design and development of the authorization and account management processes shall be defined through the [ISO] and managed through the [Insert Appropriate Department] Help Desk.

**Help Desk** – The help desk, under the direction of the [ISO] is responsible for account management and maintenance of access privileges across the [LEP] application portfolio as well as notifying the appropriate [Data Owners] of any access concerns or issues.

### ACCESS CREDENTIAL MANAGEMENT

Account requests shall be processed through a standard procedure and process across [LEP]. [Insert Appropriate Department] shall define and manage this process on behalf of the [LEP] through the {LEP] helpdesk and support/ticketing system. The following requirements shall be enforced:

* Access requests shall be limited to the systems and applications described on the work order
* Applications shall only be used for the purposes stated on the request
* A new request is required if there are changes in role or access privilege to the stated application
* The authorization request must be approved by the [Data/Application Owner]

Access to systems and applications are generally established or reviewed under the following conditions:

* A new User requires access for the purpose of fulfilling job responsibilities
* An existing User has a change in job function requiring a change in role and privileges
* A User is terminated or no longer needs access to the system or application

Requests for a change in access rights (e.g., to grant or disallow access) shall be accomplished by submitting a new help desk request following account management procedures and processes defined by the [LEP].

### TRANSFERS, TERMINATIONS, MAINTENANCE, AND DATA RETENTION/TRANSFER

The following processes and procedures shall be followed when a [User] transfers, retires, is terminated, or otherwise removed from the organization:

* When a User is transferred or terminated, access to systems and applications shall be immediately terminated unless justified and approved in writing by the [Data Owner] and [ISO]
* User work records and data stored locally or on [LEP] servers shall be preserved
* The process for system and account revocation is managed through the [ISO] and [Insert Appropriate Department] in concert with application data owners and [LEP] management
* It is the responsibility of the direct supervisor or manager to notify all appropriate personnel when a [User] transferred or terminated
* The [Data Owner] for each information system shall ensure that all user accounts are reviewed and access rights evaluated at least once per year
* Account databases shall be regularly scavenged for inactive records and disabled as appropriate based on a schedule for account maintenance determined by the [ISO]

### ACCESS SECURITY MECHANISMS

User identification and authentication is defined as an access control methodology. [LEP] uses strong passwords, group policy, Single Sign On (“SSO”), and secure two-factor authentication wherever possible to determine a user’s identity, ensure it is correct, and establish accountability. User login IDs and password shall be unique and not be shared by [Users] through the use of generic accounts. Passwords are required to meet strong authentication requirements and all application access shall be based on the role of the user in the system, granting access to the minimum amount of information necessary for the User to accomplish job functions.

### ADMINISTRATION AND MANAGEMENT

**[Information Security Officer]** - The [ISO] or their designee shall ensure that:

* All default user passwords are changed at the first login
* Default application, database, and system passwords shall be changed by systems personnel before moving into production
* Default user accounts provided with purchased software must be disabled or the account names changed upon installation
* Default accounts must be used only for designated maintenance tasks and must not be employed for daily use
* Security mechanisms shall restrict access to credentials for the least privilege necessary to perform job responsibilities and such access is based on job classification role and function
* Approvals are secured by authorized parties specifying necessary access control lists
* Access control lists for systems components shall be set to deny all unless privilege to a particular function is explicitly allowed
* Termination procedures exist for handling data and they are well known by support staff and [LEP] [Insert Appropriate Department]
* Procedures exist that assign responsibility for removing IT and/or physical access to facilities and collection of premise keys, cards, and other mechanisms for secure facility access
* Regular reviews of [Users] with access to sensitive information shall be performed to ensure they are appropriate, necessary, and valid
* Inactive accounts shall be immediately disabled or removed from account databases
* The organization assigns a unique name and/or number for identifying and tracking user and administration identity. Procedures require that:
  + User identifiers be in a specific format and singularly unique
  + Identifiers be used to track activity within information systems that contain sensitive information
  + Authentication procedures verify identity
  + Policies defined by the [ISO] shall specify the types of approved authentication mechanisms that are reasonable and appropriate and control the addition, deletion, and modification of [User] credentials and other identifier objects
* Helpdesk staff shall employ at least one of the following methods defined by the [ISO] to determine the identity of an individual requesting support
* Shared or guest accounts shall not exist for system administration or generic roles/usage or other functions excepting identified service account credentials managed, defined, and documented by [LEP] [Insert Appropriate Department]
* Configuration standards are developed for all system components. Such standards shall:
  + Address known security vulnerabilities
  + Be consistent with industry accepted system hardening standards recommended by the Center for Internet Security (CIS), International Standards Organization (ISO), SysAdmin Audit Network Security (SANS), and National Institute of Standards Technology (NIST)
  + Ensure that security policies and operational procedures for managing application default accounts, system accounts, and other security parameters are documented, in use, and known to all affected parties
  + Ensure two-factor authentication is implemented for remote network access originating from outside the network by all staff and all third party providers, (including vendor access for support or maintenance)

**End-User Support and Helpdesk Staff** – [LEP] support and helpdesk staff shall ensure:

* Vendor supplied default credentials are modified, removed, or disabled
* Unnecessary default or generic accounts are changed before system on the network, including firewalls, routers, servers, storage devices, wireless devices, etc. that are connected to sensitive data or used to transmit sensitive data
* Ensure all default passwords are changed including, but not limited to, those used by operating systems, software that provides security services, application and system accounts, Point-of-Sale (“POS”) terminals, Simple Network Management Protocol (“SNMP”) community strings, etc.)
* Change wireless vendor defaults for environments containing or transmitting sensitive data, including, but not limited to, default wireless encryption keys, passwords, and SNMP community strings
* Account creation and control shall be governed by this policy and the [LEP] Access Control and Password Policy
* Accounts of individuals on extended leave (more than 30 days) shall be disabled
* All new user accounts not been accessed within 60 days of creation will be disabled
* Existing accounts not accessed for a period of 90 days will be disabled and deleted from the account database if not accessed after 180 days

**Network Administration and Support** - System administrators or other designated staff shall ensure:

* A documented process exists to modify accounts that accommodates situations such as name changes, accounting changes, and/or permission changes
* Periodic reviews of existing accounts for validity on a scheduled set forth by the [ISO]
* All actions and systems are available and staff cooperate with independent audit reviews for compliance
* Account listings and other controls are reported as requested by authorized management
* Staff cooperate with authorized [LEP] management during security incident investigations
* Server roles and functions are organized and partitioned to appropriate functions and services that limit access risk (for example, web servers, database servers, and Domain Name Servers (“DNS”) should be implemented on separate systems)
* Where virtualization technologies are in use, the administrator shall implement only one primary function per virtual system component
* Only necessary services, protocols, daemons, etc., required for the function of the system are enabled and all unnecessary features or unsecure features are disabled (NetBIOS, Telnet, FTP, etc.)
* Any additional security features required for services, protocols, or daemons that are considered to be insecure are implemented (for example, use of secured technologies such as SSH, SFTP, SSL, etc. to protect unsecure services)
* System security parameters and group policies are appropriately configured to prevent misuse and limit access to local consoles
* All non-console administrative access using strong cryptography are encrypted
* Inventory of infrastructure assets and related functions are maintained
* Identity is verified before modifying authentication credentials or security access

### USER NOTIFICATIONS

[Users] of information systems shall be notified either in writing or through electronic means whenever:

* Gaining access to a system where usage is monitored, recorded, and subject to audit
* Logging into [LEP] systems via Active Directory security notification/splash screen and that [User] has granted consent to such monitoring and recording
* Unauthorized use is prohibited and subject to criminal and civil penalties

### OTHER CONSIDERATIONS

Security personnel shall ensure effective administration of computer access to maintain system security. The following are important administrative considerations:

**Audit and Management Reviews** – On an annual basis, [ISO] and management personnel shall review system user account documentation for compliance. These reviews shall be conducted on a system wide basis. Reviews should examine:

* Levels of access
* Conformity with the concept of least privilege
* Accounts scavenging practices
* Appropriate documentation and authorizations are secured

**Detecting Unauthorized/illegal Activities** – Alternative mechanisms shall be used to detect unauthorized and illegal acts. The [ISO] and [CIO] shall determine the mechanisms and tools used to assist in managing premise, network, and system security.

**Staff Terminations** - Termination of staff shall be classified as either friendly or unfriendly.

* *Friendly Terminations* – These events shall be accomplished by implementing a standard set of procedures and protocols for individuals. All termination work shall be coordinated through [LEP] [Human Resources]. This normally includes:
  + Removal of access privileges, computer accounts, authentication tokens
  + The control of keys to the office and/or office furniture and equipment
  + The briefing on the continuing responsibilities for confidentiality and privacy
  + Return of any [LEP] property
  + Interim or replacement staff’s ability to access data

***Unfriendly Terminations*** – These events have the potential for adverse consequences. All termination work shall be coordinated through [LEP] [Human Resources]. As such the following protocols shall be observed:

* + System access shall be terminated to all systems as quickly as possible
  + If staff are immediately terminated, system access shall be removed at the same time (or just before) the individual is notified and dismissed. Coordination of the event shall occur through [LEP] [Human Resources]
  + Staff shall return all items or assets that belong to [LEP]
  + All actions should be performed in accordance with [Insert Appropriate Department] leadership and direction
  + Assets shall be held as instructed in the case of legal review, chain of custody, or other investigative events. Legal holds shall be communicated by [LEP] [HR] through the [CIO] and [ISO]

## **Audit Controls and Management**

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of the [LEP]. Satisfactory examples of evidence and compliance include:

* Unit procedural and process documentation with roles and responsibilities
* Security logs detailing system and application access events
* Documented account creation, scavenging, deletion, and other procedures outlined in this policy in use by [Insert Appropriate Department] support staff
* Historical and archival correspondence around policies and procedure outlined in this document

## Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

## Distribution

This policy is to be distributed to all [LEP] staff supporting application and system security.

## Policy Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 11/30/2016 | Initial Policy Drafted |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |