# Access Control and Password Policy

## Overview

Computer accounts are used to manage security privileges and grant access to [LEP] information systems and applications. The process of creating, controlling, managing, and monitoring computer accounts is critical to a comprehensive security program.

## Purpose

Identification and authentication access controls play an important role in helping to protect information systems and the data contained within them. The purpose of this policy is to define requirements, procedures, and protocols for managing access control and passwords within the [LEP].

## Scope

This policy applies to all [LEP] staff, users, and contractors that use, create, deploy, or support application and system software. This policy applies to all computer assets and software regardless of ownership.

## Policy

### GENERAL

The [Insert Appropriate Role] or their designee shall ensure that policies and procedures exist to:

* Manage the process of creating, changing, and safeguarding passwords/phrases
* Prevent staff from sharing passwords/phrases with others
* Advise staff to commit their passwords/phrases to memory and not allow them to be written down
* Govern password/phrase change frequency
* Dictate when passwords/phrases must be supplemented with additional access controls such as “smart” card, tokens, or other supplemental two and/or three factor authentication verification procedures

This Policy applies to all [LEP] related authentication activities including but not limited to the following types of computer hardware, application, and device based accounts:

* Systems administrative
* Role-based administrative
* End-user accounts
* Network infrastructure devices (e.g. firewalls, routers, wireless access points, etc.)
* Third party service providers
* Web applications
* Screen savers
* Mobile devices

### NEW USER ACCOUNTS

When creating and granting access for a new end user account:

* System administrators shall establish a unique ID and unique password/phrase separate from their regular user account
* End user passwords will be conveyed to staff and customers in a secure manner
* End users will be required to change their initial password/phrase to something that adheres to policy and is known only to that user

### SELECTING PASSWORDS/PHRASES

All users shall select passwords/phrases that meet requirements for being strong and complex. Staff shall be required to choose passwords/phrases that meet the following requirements:

* Contain both upper and lower case characters (e.g., a-z, A-Z)
* Include both numbers (0-9) and special characters (e.g. @, #, $, \*)
* Have a minimum of at least 8 characters (preferably 10 characters long or more) and are phrase based
* Where possible, use different passwords/phrases for general office activities (e.g. e-mail, file access) vs. systems that store sensitive or confidential data

Password attributes shall be enforced through a directory service password group policy applied at the [LEP] enterprise level. Staff shall not choose passwords/phrases that:

* Include common words found in a dictionary
* Are the same as passwords/phrases used on personal accounts (e.g. email, online banking, or social media)
* Contain personal information such as a spouse or pet’s name, Social Security Number, driver's license number, street address, phone number, etc.
* Contain sequences or repeated characters (1234, 3333, etc.)

Staff with special system privileges, assigned by a transaction, program, process, or group membership, should select a unique password/phrase from other accounts held by that individual.

Generic user accounts shall not be authorized for use by staff on any [LEP] based computer applications or hardware.

### PASSWORD/PHRASE GUIDELINES

Staff shall follow this [LEP] security policy and guideline to ensure passwords/phrases are not compromised. Security training shall ensure staff are educated and reminded of:

* Security related risks of lax password procedures
* [LEP] requirements in selecting and protecting passwords/phrases
* Not selecting the "Remember Me" or “Remember Password” feature in web applications and browsers
* Cautions when using social media so a password/phrase combination is not compromised

Additionally, passwords and passphrases must not be:

* Revealed or shared with any other individual
* Stored, written down, or transmitted in clear (unencrypted) text
* Inserted into unencrypted email messages or other forms of electronic communications

Should a staff member believe their password/phrase has been compromised or made available to others, they must immediately reset/change their password and notify [LEP] [Insert Appropriate Role/Department].

### PASSWORD/PHRASE CHANGES

Passwords/phrases shall be changed on a regular basis according to the following schedule:

* Administrative passwords/phrases must be changed at least every 60 days.
* User passwords/phrases must be changed at least every 90 days.
* Staff shall not repeat any of their prior five passwords/phrases.

These password policies shall be enforced through a directory service password group policy applied at the [LEP] enterprise level.

### SOFTWARE APPLICATIONS

Application developers must ensure programs contain the following security precautions:

* Applications must require each end user to have their own unique user ID (e.g. generic, shared, service, or group based accounts are disallowed). It is acceptable to use security groups for access control lists to certain features and functions of an application
* Passwords/phrases and sensitive information shall be protected using at-rest and in-transit encryption
* Passwords/phrases and sensitive information shall not be transmitted or stored in clear text
* Application timeout standards shall be enforced and require a user to re-enter a password/phrase after a period of inactivity to regain access to their application

## **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] internal application development and release methodology. Examples of control procedures shall be demonstrated through regular and repeatable administrative processes as follows:

* Documented and formalized account provisioning procedures.
* Documented and demonstrable access control group policy around strong password and history requirements.
* Annual audits of directory accounts for ‘dead’ account scavenging process.
* Documented process for long-term and short-term employee/contractor classes.
* Appropriate logging, alerting and reporting of security events within applications and server based access.

## 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 and contractors using [LEP] information resources.

## Policy Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 09/12/2016 | Initial Policy Drafted |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |