# Administrative Special Access Policy

## Overview

Technical support staff, security administrators, system administrators, and others may have need for special account access priviledges compared to typical or everyday users. The fact that these administrative and special access accounts have a higher level of access means that granting, controlling, managing, and monitoring these accounts is extremely important to [LEP]’s information security program.

## Purpose

The purpose of this policy is to establish policy and procedure for creating, using, monitoring, controlling, and removing accounts with special access privileges.

## Scope

This policy applies to all [LEP] staff members that have or may require special access privileges to information resources, systems, and/or facilities.

## Policy

All [LEP] units shall annually submit to the [Insert Appropriate Role] or their designee a list of administrative contacts for their systems that connect to network special access or system accounts. The following account access provisions shall be followed:

* Users of administrative/special access accounts must have and follow all pertinent account management policies, procedures, documentation, training, and authorizations
* Each individual that uses administrative/special access accounts must refrain from abuse of this privilege and must only do so for administration of [LEP] resources, investigations, or other specialized roles under the direction of executive management, the [Insert Appropriate Role or Roles]
* Individuals using administrative/special access accounts must use the account privilege most appropriate for the work performed (e.g. user account vs. administrator account)
* Each account used for administrative/special access must comply with applicable [LEP] policy
* Passwords for shared administrator/service and special access accounts must change when an individual with the password leaves [LEP] or upon a change in the vendor contract personnel assigned to a contract
* In the case where a system has only one system administrator, there must be a password escrow procedure in place so that someone other than the administrator can gain access to the administrator account in an emergency situation

When special access accounts are needed for audits, software development, software installation, or any other defined/authorized need, they must be:

* Properly initialized and authorized
* Created with a specific expiration date
* Adhere to all [LEP] account security policies
* Disabled and/or removed when work is complete

## Audit Controls and Management

On-demand documented procedures and workplace evidence of regular management practice should be in place for this operational policy. [LEP] should maintain a historical log of special access and authorization practice and periodically review actual performance against policy.

## 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 | 8/30/2016 | Initial Policy Drafted |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |