Tier 1 Control Standards (State-Wide)

Elevated Account Access Controls

Standard ID
IOT-CS-SEC-118

Published Date
3/12/2010

Effective Date
3/27/2010

Last Updated
2/5/2018

Next Review Date
2/5/2019

Policy
06.0 Access Control (PR.AC)
  06.1 PR.AC-1
  06.1.1 Account Management

Purpose
To define requirements related to the authorization and use of elevated accounts.

Scope
IOT Supported Entities

Statement
An elevated account is one in which non-standard access rights, rights providing additional access and capabilities, are assigned to individuals on network infrastructure such as servers and routers or groups of workstations. Elevated accounts are to be used only for duties requiring the additional permissions. Non-administrative tasks should be performed with standard access. Below are the additional requirements for elevated accounts:

- Any account with elevated privileges must be authorized by the agency.
- Passwords must meet complex criteria and contain a minimum of 8 characters
- Passwords must be changed every 60 days
- Restrictive controls will be placed on elevated accounts to prevent access to the Internet
- Restrictive controls will be placed on elevated accounts to prevent access to email or the use of mailboxes unless required for alerting purposes.

Roles
Agency Management
IOT Personnel
Users with Elevated Privileges

Responsibilities
Elevated account users shall only use the account for duties requiring the additional permissions. Non-administrative tasks should be performed with standard access. IOT shall create a second account to be used for tasks requiring non-standard, elevated access.

Management Commitment
Management shall approve elevated privileges based on least privilege, and actively review this access periodically.
Coordination Among Organizational Entities
Agencies shall coordinate with IOT if elevated access is needed.

Compliance
Access to Internet or connections to mail protocols using elevated accounts will be monitored and reported to IOT and agency leadership.

Exceptions
No exceptions.