Tier 1 Control Standards (State-Wide)

Access Control

Standard ID
IOT-CS-SEC-138

Published Date
7/1/2015

Effective Date
7/1/2015

Last Updated
5/17/2017

Next Review Date
5/17/2018

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

06.1.1 Account Management

Purpose
This Standard summarizes the access controls for which compliance is required for systems containing confidential information.

Scope
IOT Supported Entities

Statement
The following controls are required for confidential systems:

Account Management

- All accounts are role based with the rights for each clearly documented.
- Access will be granted to the system only with approval from the system owner. Agencies shall establish a reliable process ensuring only those requiring access obtain access and that the access is limited to only those accesses needed to complete their duties.
- Temporary accounts will be established only when short term technical support is needed on the system. All access must be auditable to an individual. Generic or shared accounts are prohibited for confidential systems.
- Access for all accounts shall be terminated immediately when no longer needed.
- Accounts will be monitored every six months, by the system owner or auditor, to ensure all are in use, appropriately limited by role, and that timely termination occurred.
- System owners and auditors shall be notified in regard to elevated privilege account creation, modification, disabling and termination actions.
- Service accounts will be documented and limited in regard to their purpose.
- Default accounts will be renamed or eliminated.

System Access

- Each role defined will have the minimum access to data required to complete their duties.
- Elevated privilege accounts are to be used solely for administration duties requiring the special access. Elevated accounts shall not be used for routine productivity functions such as email, document generation (e.g. – Word, Excel, etc.), Internet surfing, and other functions.
• Elevated accounts shall be distinct and unique from agency to agency when the agency has isolated its systems from others on the network.
• Login ID and passwords will be gained through Active Directory or an access management system selected by the state (an encrypted, FIPS 140-2 and NIST validated module).
• Elevated privilege passwords will have a minimum of 14 characters.
• Wireless access directly to a confidential system by those with elevated privileges is prohibited.
• Remote access directly to a confidential system from an elevated privilege account is prohibited.
• The system owner shall audit elevated privilege access, both successful and unsuccessful, based on criteria defined to be potentially indicative of attempted unauthorized access.
• A session lock will be initiated after 15 minutes of inactivity.

Information Flow Enforcement

• Prior to isolation, approved information system flows shall be diagramed and documented. This documentation will be reflected in firewall settings. The documentation must be updated whenever approved system information flows change.
• Auditing will be established for system events. Events will be funneled to the SIEM in order to identify unauthorized flows of information.

Separation of Duties

• Access to the system and system log files shall be appropriately limited and segregated by role.

Roles
Information Asset Owners/System Owners

Responsibilities
Information Asset Owners/System Owners shall maintain access control for each confidential system in accordance with the requirements written within this Standard.

Management Commitment
Management is responsible for ensuring their agency is meeting the requirements written within this standard.

Coordination Among Organizational Entities
Agencies shall coordinate with IOT where necessary to appropriately secure confidential systems as it pertains to this Standard.

Compliance
Compliance activities will be system dependent but general requirements are identified in the control section above.

Exceptions
No exceptions.