Tier 1 Control Standards (State-Wide)

Identification and Authentication

Standard ID
IOT-CS-SEC-141

Published Date
7/1/2015

Effective Date
7/1/2015

Last Updated
5/19/2017

Next Review Date
5/19/2018

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

Purpose
This practice summarizes the user identification and authentication in place for State systems with confidential data.

Scope
All Devices that Connect to the State Network

Statement
The following controls are required for confidential systems:

- Each system user and device is uniquely identified. Identifiers are not reused.
- Each user authenticates through a means that includes a secret only they know (e.g. – a password)
- Any service processes in the system are conducted through service accounts and not through individual user IDs
- Service accounts are limited to their specific purpose, their purpose is documented, and their passwords are set to the state’s standard setting for service account password strength
- Only devices included in the documented system design are authorized to access the system. New devices must be approved through change control complete with an updated design and demonstrated to be compliant with the controls specified in the configuration management policy.
- Passwords for elevated accounts will have a 14 character minimum with a complex makeup. Passwords are encrypted in storage and in transmission
- Passwords may not be reused and new passwords must include a minimum of 4 changed characters
- All passwords will have a minimum lifetime of 1 day
- The system obscures the password as it is entered into the system for authentication
- Authentication is through an encrypted, FIPS 140-2 and NIST validated cryptographic module
- Only users expressly identified and authorized shall access the system.
Roles
All Personnel

Responsibilities
All personnel are responsible for maintaining identification and authentication practices commensurate with 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 to validate confidential systems are meeting this Standard.

Compliance
Agencies shall attest to their compliance with these policies on an annual basis providing evidence as directed by the auditor or the CISO.

Exceptions
No exceptions.