Tier 1 Control Standards (State-Wide)

Security Assessment and Authorization

Standard ID
IOT-CS-SEC-146

Published Date
7/1/2015

Effective Date
7/1/2015

Last Updated
5/19/2017

Next Review Date
5/19/2018

Policy
04.0 Risk Assessment (ID.RA)
04.6 ID.RA-6
04.6.1 Risk Response

Purpose
This Standard summarizes the security and assessment authorization controls in place for confidential systems.

Scope
IOT Supported Entities

Statement
The following controls are required for confidential systems:

Assessment

- System owners shall ensure an assessment of security controls. The assessment will be part of a continual process performed by trained staff capable of determining the effectiveness of controls.
- The system will be assessed bi-annually by an outside, independent and appropriately qualified assessor.
- An annual report will be provided to the system owner, agency leadership and the State CIO. The report will not be a public document or shared broadly due to the confidential nature of the system.
- A Plan of Action and Milestones (POA&M) will be developed within 30 days of the final results from the assessment and/or penetration test. The POA&M will be managed and updated until all findings are resolved.
- Connections with other systems will be assessed and approved and documented in a Memorandum of Understanding. Each connection, the interface characteristics, security requirements, and the nature of the information communicated will be documented.

Authorization

- The agency head or their designee shall authorize operation of each system with confidential data and explicitly accept the risk to organizational information assets.
- Systems will be authorized before going live, after significant changes to the system, and, at minimum, every three years thereafter.
• The system will be continuously monitored to maintain the system authorization. Appropriate tools will be used to address threats and vulnerabilities through the system’s lifecycle.

Roles
Agency Executive Management
Information Asset Owners/System Owners

Responsibilities
Information Asset Owners/System Owners shall assess risk to their systems and mitigate risk to appropriate levels of acceptable

Management Commitment
Management is responsible for ensuring their agency appropriately classifies systems and takes the necessary actions defined in this

Coordination Among Organizational Entities
Agencies shall coordinate with IOT where implementation of security configurations cannot be performed by the agency.

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

Exceptions
No exceptions.