Tier 1 Control Standards (State-Wide)

Program Management

Standard ID
IOT-CS-SEC-145

Published Date
7/1/2015

Effective Date
7/1/2015

Last Updated
5/19/2017

Next Review Date
5/19/2018

Policy
09.0 Information Protection Processes and Procedures (PR.IP)
  09.7 PR.IP-7
  09.7.1 Information Protection Metrics and Improvement

Purpose
This Standard summarizes the program management requirements for the systems with confidential data.

Scope
IOT Supported Entities

Statement
The following controls are required for confidential systems:

- Agencies shall ensure appropriate funding and resources are invested in the security of their systems with confidential data.
- Systems are self-assessed for compliance with policy and standards. Shortcomings are identified and tracked for progress toward compliance.
- Systems are assessed by independent third parties with the interval between assessments no greater than 2 years.
- Security metrics for systems are identified, tracked and published.
- The system owner ensures appropriate risk management strategies are in place and implemented consistently.
- Roles in the assurance of system security are clearly defined.
- System authorization is given by the agency head or their designee through a formal process and filed with the State CISO for review by the CIO and oversight bodies.

Roles
Agency Executive Management
Information Asset Owners/System Owners

Responsibilities
Information Asset Owners/System Owners must appropriately manage confidential systems by meeting the defined requirements written within this Standard.
Management Commitment
Management shall authorize

Coordination Among Organizational Entities
Agencies shall coordinate with IOT where necessary to appropriately secure data in accordance with 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.