Tier 1 Control Standards (State-Wide)

System and Services Acquisition

Standard ID
IOT-CS-SEC-149

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)
  09.2 PR.IP-2
  09.2.1 Secure System Development Life Cycle

Purpose
This Standard summarizes the system and services acquisition requirements for systems with confidential data.

Scope
IOT Supported Entities

Statement
The following controls are required for confidential systems:

- The system inclusive of all its components are documented.
- External systems connections are limited to only those needed for system functionality. These connections are identified and white listed while others are blocked.
- Application software shall be purchased only from reputable vendors with a proven capability of delivering and maintaining secure products. Systems with Internet facing components shall be assessed by independent third parties before being placed in production and every two years going forward.
- Custom developed code or scripts used as part of the system shall be tested for vulnerabilities prior to initial implementation and as part of the change control process.
- Hardware and software comprising the system shall be examined for appropriateness in terms of their security capabilities referencing government standards and approved vendor lists.
- Software usage is in compliance with contract agreements and copyright laws.
- No user installed software is permitted without express agency authorization. All software must be inspected and approved by the system owner.

Roles
Agency Management
Information Asset Owners/System Owners

Responsibilities
Information Asset Owners/System Owners must be vigilant in documenting, tracking and validating system components use and meet 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 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.