Tier 1 Control Standards (State-Wide)

Information System Inventory

Standard ID
IOT-CS-SEC-101

Published Date
9/27/2006

Effective Date
9/27/2006

Last Updated
5/30/2017

Next Review Date
5/30/2018

Policy
01.0 Asset Management (ID.AM)
01.2 ID.AM-2
01.2.1 Software Inventory

Purpose
An Information System Inventory (ISI) application has been developed to assist agencies with the tracking of their manual and automated systems. It is a requirement that all state agency systems be entered into the database. Separately elected officials may use the application as they desire. The inventory is generally static in nature but very important to keep current. It eases identification of systems containing personal information needed for reporting as well as data categorization that drives system designs, disaster recovery, and security requirements.

Scope
IOT Supported Entities

Statement
System owners shall obtain the appropriate access to the ISI to complete duties:

- Owners access only those systems for which they are responsible; assuring each field is complete and accurate
- Owners confirm that system availability and confidentiality (security) requirements are properly supported at a level consistent with the system's categorization
- Data categorization changes must be reflected appropriately in adjustments to SLAs, disaster recovery plans, and/or security levels.

Roles
Information Asset Owners/System Owners

Responsibilities
System owners shall ensure that information in the ISI is current and complete. IOT shall ensure maintenance of the database and reporting on behalf of agencies to the Legislature and Governor's Office.

Management Commitment
Management shall ensure that all relevant systems are documented and updated in the ISI in accordance with this standard.
Coordination Among Organizational Entities
Agencies shall notify IOT of any issues with the ISI.

Compliance
IOT will check systems for availability requirements by comparing it to coverage under the IOT disaster recovery plan. No direct compliance activities result from this practice. However, reports on confidential systems will be generated annually for the Legislature and Governor’s Office. Complete and accurate information reported to these bodies is required by law. Additionally, data categorization will be regularly compared to the disaster recovery plans to assure completeness.

Exceptions
No exceptions.

Associated Links
Https://grc.iot.in.gov/rsaarcher