Tier 1 Control Standards (State-Wide)

Configuration Management

Standard ID
IOT-CS-SEC-140

Published Date
7/1/2015

Effective Date
7/1/2015

Last Updated
5/17/2017

Next Review Date
5/17/2018

Policy
09.0 Information Protection Processes and Procedures (PR.IP)
  09.1 PR.IP-1
  09.1.1 Configuration Management

Purpose
This practice summarizes the configuration management access controls in place for Indiana government Executive Branch systems containing confidential data.

Scope
All Devices that Connect to the State Network

Statement
The following controls are required for confidential systems:

- All system components are identified and inventoried.
- Each component shall be securely configured per a standardized, uniform build, documented and regularly audited for compliance with DISA Stigs.
- Agencies shall ensure that system components are compliant with DISA stigs or accept the additional risk of their systems not being hardened to the standard.
- Agencies are responsible for monitoring for STIG compliance on an ongoing basis. Change control is used to ensure configurations remain hardened to standards. Changes are tested, validated, authorized and documented before they are made operational.
- The aggregation of various components comprises the system baseline. The baseline system is documented and maintained. Changes result in the creation of a new baseline.
- The system baseline is reviewed and updated no less than annually and when major system changes are made.
- Older revisions of the system baseline are maintained to support a rollback if necessary.
- Software on the system is expressly authorized by the agency and documented as part of the configuration. Unauthorized software is prohibited and prevented from execution. This prohibition is technically enforced and can only be changed through the change management process.
- Changes to the configuration are evaluated for security impact. Negative impacts to security require authorization by agency leadership and are filed with the CISO for review by the CIO and oversight bodies.
- Security functions within the configuration are thoroughly tested then verified for producing desired outcomes after changes are implemented.
• Logical and physical access restrictions are documented, approved and enforced for all system changes. Changes to access restrictions are recorded and maintained.
• Vulnerability scans are conducted at regular intervals on the system. Vulnerabilities are remediated or the risks from non-compliance are accepted by the agency.

Roles
Information Asset Owners/System Owners

Responsibilities
Information Asset Owners/Systems Owners shall securely configure confidential systems consistent with 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 apply appropriate configurations to the confidential system(s).

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

Exceptions
Exceptions shall be filed as directed in the policy.