# P.04

## Policy Name

Configuration Management Policy

## 1. Purpose

The purpose of this Policy is to provide assurance that the systems and assets in the State Enterprise are systematically controlled and that accurate and reliable information about those systems, assets, and their associated configurations is available when needed.

## 2. Scope

The Statewide IT Policies and Standards ("POLICIES") apply to all IOT-supported entities ("Entities"), their employees, their contractors, their consultants, and their vendors. Unless otherwise specified, all of the POLICIES apply equally to physical and electronic assets and resources assigned to an individual, on-premises physical assets, on-premises virtual assets, on-premises cloud assets, assets provided by cloud service providers, products and/or services that use cloud computing, all data stored or processed by the above assets in electronic, paper, or any other form, and everything else that supports the functioning of State government ("State Enterprise").

## 3. Policy

### 3.1 Configuration Management

a. IOT must establish and maintain a secure configuration process for enterprise assets (e.g., endpoints, network infrastructure, cloud assets, storage arrays, servers).
b. IOT and Entities should harden systems and assets according to industry security standards and manufacturer recommendations.
c. IOT and Entities should maintain records of configuration settings within the associated secure configurations guidelines and, where available, the associated Configuration Management Database ("CMDB"). IOT should review this information annually and update it when necessary.
d. IOT and Entities should list all systems and assets in the CMBD, including network and cloud assets.

### 3.2 Baseline Configuration

a. Hardened baseline configurations should provide a commensurate level of security in alignment with the specific asset or system criticality rating.
b. IOT and Entities must apply hardened baseline configurations to systems and assets before connecting to the State network.
c. IOT and Entities should use secure, nondeprecated network management protocols, such as Secure Shell ("SSH"), Hypertext Transfer Protocol Secure ("HTTPS"), and a nondeprecated version of Transport Layer Security ("TLS") to manage enterprise assets and software.
d. Assets hosting sensitive data should require additional security controls (e.g., penetration tests, static code analysis) as part of the initial platform development.
e. IOT and Entities should follow least privilege in selecting configuration settings by allowing users to have only those capabilities necessary for their roles, including the disabling of unnecessary services.
f. IOT and Entities should establish, document, implement, and monitor mandatory configuration settings for assets using a security configuration checklist that reflects the most restrictive mode, consistent with operational requirements.
g. IOT and Entities must configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed fifteen minutes. For mobile enduser devices, the period must not exceed two minutes.
h. IOT and Entities should enforce automatic device lockout following a predetermined threshold of local, failed authentication attempts on portable end-user devices. For laptops, do not allow more than twenty failed authentication attempts. For tablets and smartphones, do not allow more than ten failed authentication attempts.
i. IOT and Entities should include the capacity of remotely wiping portable end-user devices.

### 3.3 Applying Configuration Settings

a. IOT must establish and document a golden image or secure build of systems and assets for workstations, servers, and network equipment. This should include trusted or enterprise-controlled Domain Name System ("DNS") servers.
b. To protect the integrity of the image, golden images should be stored in a secure location that is only accessible by individuals with a business need.
c. All purchased, vendor-configured systems must have appropriate configuration documentation, including baseline configuration details when possible.
d. Asset configuration privileges should be limited to administrators with valid authority.
e. IOT must account for default manufacturer settings and accounts and change default credentials.

### 3.4 Applying Cloud Configuration Settings

a. When applicable and feasible, a baseline image must be established for cloud resources and infrastructure.
b. Configuration settings and changes related to cloud infrastructure and assets (e.g., compute, network, and storage) must be evaluated based on State and Federal requirements.
c. Cloud configuration management must follow the benchmarks required by the cloud service provider based on the shared responsibility model.

### 3.5 Change Control and Plan Management

a. Configuration changes must be documented and approved as part of the change management process prior to implementation. See the Change Management Policy for more information.
b. IOT and Entities should maintain previous configurations to support a secure rollback.

## 4. Exceptions

Exception Requests will be addressed through the process designated by IOT.

## 5. Ultimate Authority

The Chief Information Officer is the ultimate authority for decisions made pursuant to the POLICIES, including Exception Requests.

## 6. Roles and Responsibilities

State agencies vary tremendously. Some State agencies have Chief Information Officers, while others may have no dedicated IT employees. Because of that variance, the Statewide IT Policies and Standards do not refer to a specific job title as being responsible for compliance. Instead, the intent is for the responsibilities to rest with the agency head or the highest-ranking employee responsible for IT, unless stated otherwise regarding a specific duty.

## 7. Statutory Purposes

The statutory purposes of IOT include "establish the standards for the technology infrastructure of the state" and "provide for the technology and procedures for the state to do business with the greatest security possible," Ind. Code § 4-13.1-2-1(1) and (5). IOT has an obligation to "develop and maintain policies, procedures, and guidelines for the effective and secure use of information technology in state government," Ind. Code § 4-13.1-2-2(a)(11).

## 8. Industry Standards

The Statewide IT Policies and Standards are based on the following:

Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, U.S. National Institute of Standards and Technology, Special Publication 800-37 Rev. 2. https://csrc.nist.gov/pubs/sp/800/37/r2/final

Security and Privacy Controls for Information Systems and Organizations, U.S. National Institute of Standards and Technology, Special Publication 800-53 Rev. 5. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

Critical Security Controls v.8.1, Center for Internet Security. https://www.cisecurity.org/controls

## 9. Federal Audit

The federal government audits the IT practices of several Entities. Where necessary, those Entities may create agency-specific policies to supplement the Statewide IT Policies and Standards. Those agencies include the Bureau of Motor Vehicles, Department of Child Services, Department of Revenue, Department of Workforce Development, Family and Social Services Administration, Indiana Office of Technology, and the Indiana State Police.