

	<b>Department of Administration</b>  <b>Policy</b>	Category	<b>Configuration Management, SITSD Security</b>
		Effective Date	<b>01/01/2010</b>
		Last Revised	<b>09/17/2014</b>
Issuing Authority	<b>State Information Technology Services Division</b>		
<b>POL-Configuration Management Policy</b>			

### I. Purpose

The purpose of this Policy is to establish the requirement for the State Information Technology Services Division (SITSD) to implement Configuration Management for information systems that SITSD manages or controls.

### II. Scope

This Policy encompasses information systems that SITSD manages or controls, including systems that third-parties manage or host on SITSD's behalf.

### III. Policy Statement

SITSD shall develop and implement Configuration Management for the state's enterprise information systems maintained by SITSD based on the [National Institute of Standards and Technology \(NST\) SP800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations](#), and associated NIST guidelines and standards.

### IV. Roles and Responsibilities

The following roles and responsibilities are required by this policy:

- A. Chief Information Officer:** Oversees the information technology resources that maintain information systems for SITSD.
- B. Chief Information Security Officer:** Ensures compliance with security policies and procedures within SITSD.
- C. Chief Technology Officer:** Monitors organization compliance and may make enforcement recommendations to the appropriate level of management given the particular circumstances.

- D. Chief Intergovernmental Relations Officer:** Monitors organization compliance and may make enforcement recommendations to the appropriate level of management given the particular circumstances.
- E. Chief Operations Officer:** Monitors organization compliance and may make enforcement recommendations to the appropriate level of management given the particular circumstances.
- F. Chief Financial Officer:** Monitors organization compliance and may make enforcement recommendations to the appropriate level of management given the particular circumstances.
- G. Division Personnel:** Responsible for implementation of requirements that are contained in policies and procedures.

To support Configuration Management, this Policy requires that SITSD shall:

1. Implement this Policy in compliance and integrated with guidance provided by the [National Institute of Standards and Technology Guidance](#).

Configuration Management is the process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after information system implementation. Specific requirements for SITSD include:

- a. Establishing and maintaining baseline configurations and inventories of information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles using a Configuration Management Database (CMDB).
  - b. Establishing and enforcing security configuration settings for information technology products employed in information systems.
  - c. Prohibiting or restricting functions, ports, protocols and services for information systems that are identified in configuration documentation to be a risk and not necessary for the information system to function. These settings will be reviewed on an annual basis to identify and eliminate any unnecessary functions, ports, protocols, and services on information systems.
2. Establish procedures and associated supporting documents to support an information system configuration management process.
  3. Allocate adequate resources to maintain an information system configuration management process.

4. Establish and evaluate performance measures to assess implementation of this Policy, procedures, and associated documentation.
5. Review the configuration management Policy, procedure(s), and associated documents on an annual basis and make any necessary changes to provide adequate support of the configuration management process.

## **V. Definitions**

Refer to the [NIST Information Security Glossary of Key Information Security Terms](#) for a list of NIST definitions.

## **VI. Compliance**

Compliance shall be evidenced by implementing the Configuration Management Policy as described above.

## **VII. Enforcement**

Each bureau is responsible for the Policy's implementation and enforcement. The Chief Technology Officer, Chief Business Officer, and Chief Operations Officer shall monitor bureau compliance and may make enforcement recommendations to the appropriate level of management given the particular circumstances.

If warranted, management shall take appropriate disciplinary action to enforce this Policy, up to and including termination of employment, consistent with current State Policy. The discipline policy can be found in the [MOM Policy System](#) (*search for: 261*). When considering formal disciplinary action, management will consult with their assigned Human Resource Specialist before taking action.

## **VIII. References**

### **A. Legislation**

- [2-15-112 MCA](#) - Duties and Powers of Department Heads

### **B. Policies, Directives, Regulations, Rules, Procedures, Memoranda**

- SITSD Procedure: [PRO-IT Policies, Standards, Procedures and White Papers Procedure](#)

**C. Standards, Guidelines**

- [NIST SP800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations](#)