



# DEPARTMENT OF ADMINISTRATION

## Enterprise Policy

DOIT-10-14-2014

### DIVISION OF INFORMATION TECHNOLOGY

#### Configuration Management Policy

Date of Last Revision 07/31/2014

**Bijay Kumar**  
(401) 574-9220

bijay.kumar@doit.ri.gov

#### 1. Background

- a. Information systems consist of hardware and software that are networked and configured in a complex manner and are typically in a constant state of flux throughout their lifecycle in response to changes in business processes, new or updated hardware and software, vulnerability patching, security threats, etc. This state of flux requires that changes, often intricate and extensive, to information system configuration setting be made. Managing the implementation of system changes is critical to maintaining system security and reducing overall organizational risk.

#### 2. Purpose

- a. To establish a Configuration Management Policy for effectively managing risk associated with changes to and that have an impact on system configurations, baseline configuration settings, and overall information system security.

#### 3. Scope

- a. This policy covers all State Executive Branch Departments<sup>1</sup> (including agencies, boards and commissions), and its and their employees, whether permanent, non-permanent, full or part-time, and interns as well as all individuals including, but not limited to, employees, whether permanent, non-permanent, full or part-time, interns, and all consultants, contractors, vendors, contracted individuals, and any entity with access to State data or computers and systems operated by the State or maintained on behalf of the State.

#### 4. Authority

- a. Executive Order 04-06 established the Division of Information Technology ("DoIT") within the Department of Administration to improve the efficiency, effectiveness, and security of IT management and operations within the Executive Branch of the State of Rhode Island. The DoIT Chief Information Officer ("CIO") is authorized, directed, and responsible for the oversight, coordination, and development of all IT resources within the Executive Branch. DoIT will define, maintain, and enforce State-wide IT related policies, standards, and procedures for the effective use and security of these resources.

#### 5. Definitions

---

<sup>1</sup> State Executive Branch Departments does not include the University of Rhode Island, the State colleges, State Treasurer, the Attorney General and State Secretary of State.

- a. **Baseline Configuration** - An agreed upon set of technical, functional, and physical specifications that reflects the current information system architecture, serves as the basis for future changes, and is the foundation of Configuration Management. A baseline configuration includes, for example, standard software installed on workstations, laptops, servers, network components, and mobile devices, operating system and application versions and patch sets, and configuration settings.
- b. **Configuration Management** - The process of establishing, maintaining, and managing changes to system hardware, software, documentation, and functional and physical characteristics of the operational environment throughout the information system lifecycle.
- c. **Configuration Management Plan** - Defines system level processes and procedures for how configuration management will be implemented to support system development lifecycle activities.
- d. **Configuration Settings** - Parameters within information system hardware, software, or firmware components that may be changed and, as a consequence, have an effect on the security posture or functionality of the system.
- e. **Inventory** - A detailed, itemized list, report, or record of things associated with the system.
- f. **Security Impact Analysis** - An analysis of a proposed change to determine its potential impact on system security. The analysis may include such tasks as reviewing security plans, conducting risk assessments, and performing tests within a test environment.
- g. **Waiver** - A dispensation from policy due to extenuating circumstances.

## 6. Policy

### a. Configuration Change Control.

- (i.) Configuration settings will be established, documented, monitored, and controlled.
- (ii.) The types of changes to be placed under configuration control will be identified.
- (iii.) Proposed changes to information systems will be reviewed by appropriate personnel. A security impact analysis will be performed to determine its potential impact on system security.
- (iv.) Configuration change decisions will be documented, retained, and available for audit.
- (v.) Configuration change control activities will be coordinated by an oversight committee.
- (vi.) Physical and logical access restrictions associated with configuration changes to information systems will be defined, documented, approved, and enforced according to the principles of separations of duties and least privilege.

- b. **Configuration Management Plan.** A configuration management plan for the information system will be developed, documented, periodically reviewed, and protected from unauthorized disclosure and modification. This plan will define the roles,

responsibilities, and configuration management processes and procedures necessary for identifying and managing configuration items throughout the system development lifecycle.

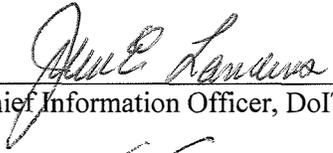
- c. **Baseline Configuration.** A current baseline configuration for each information system will be developed, documented, maintained, and periodically reviewed.
- d. **Inventory.** An inventory that accurately reflects the current information system and all of its components will be developed, documented, periodically reviewed, and updated as required.
- e. **Software.**
  - (i.) Software will be authorized and approved prior to being installed on information systems.
  - (ii.) Software and associated documentation will be used according to and tracked for compliance with contracts, licensing agreements, and copyright laws.
  - (iii.) **Policy Issuance.** This policy becomes effective upon approval and shall supersede all previously issued policies. This policy may be revoked or amended.
  - (iv.) **Policy Reviews.** This policy will be reviewed annually and updated as required.
  - (v.) **Noncompliance.** Any person or entity that violates this policy may be subject to disciplinary action up to and including termination.
  - (vi.) **Waivers.** The Agency may request a waiver from this policy by formally submitting justification for the waiver and demonstrating that compensating controls are in place to mitigate the risk. If approved, the Agency Director must accept in writing all risk to IT system resources and data associated with the waiver. Waivers require approval from and are granted solely by the DoIT Chief Information Officer. Waivers expire one year from date of issue, or upon the ending for the reason of the waiver, whichever occurs sooner, whereupon they must be renewed.

## 7. Roles and Responsibilities

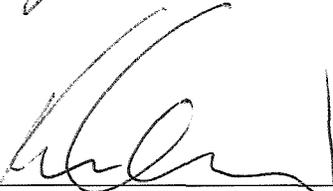
- a. *Chief Information Security Officer*
  - (i.) Periodically review and update this policy, as required.
  - (ii.) Periodically assess Agency information systems to ensure compliance with this policy.
  - (iii.) Assist in performing the security impact analysis. Review the security impact analysis.
- b. *Agency*
  - (i.) Comply with provisions documented in this policy.
  - (ii.) Develop and update, as required, a configuration management plan for each information system.
  - (iii.) Develop and update, as required, a baseline configuration for each information system.

- (iv.) Document and update, as required, an inventory of each information system.
- (v.) Perform a security impact analysis.

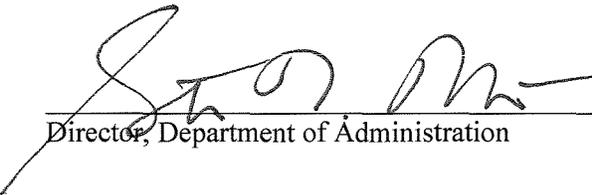
**8. Signatures**

  
\_\_\_\_\_  
Chief Information Officer, DoIT

11/25/2014  
Date

  
\_\_\_\_\_  
Chief Information Security Officer, DoIT

11/24/2014  
Date

  
\_\_\_\_\_  
Director, Department of Administration

12-3-14  
Date