

POLICY 1370.00 Information Technology Configuration Management

Issued: June 4, 2009

Revised: December 1, 2015

Next Review Date: December 1, 2016

SUBJECT: Policy for Information Technology (IT) Configuration Management.

APPLICATION: This policy is intended for statewide compliance and applies to all Executive Branch Departments, Agencies, Trusted Partners, Boards or Commissions using state of Michigan (SOM) information networks and IT Resources.

PURPOSE: This policy provides guidance for configuration management processes for new and existing IT systems within the SOM and outlines specific responsibilities for Agency Directors and the Director of the Department of Technology, Management and Budget (DTMB).

CONTACT AGENCY: Department of Technology, Management and Budget (DTMB)
Office of the Chief Technology Officer (CTO)
Infrastructure & Operations (I&O)

TELEPHONE: 517-636-6504

FAX: 517-636-6154

SUMMARY: The intent of this policy is to encourage best practices that promote the integrity and management of reliable, cost-effective, computer-based solutions.

Configuration Management (CM) is the process of identifying and defining the Configuration items (CI) in a system, controlling the release and change of these items, recording and reporting the status of CI and change requests, and verifying the completeness and correctness of CI. While the basic disciplines of CM are common to both hardware and software, these are some differences in emphasis. DTMB CM processes rely on industry standard best practices.

For operating system and hardware CM, DTMB aligns its processes with ITIL and includes the following major activities:

- Management and Planning.
- Configuration Identification.
- Configuration Control.
- Status Accounting and Reporting.
- Verification and Auditing.

For software CM, DTMB aligns its State Unified Information Technology Environment (SUITE) processes with the Capability Maturity Model Integrated (CMMI) published by the Software Engineering Institute of Carnegie Mellon University. CM activities within CMMI include:

- Establishing baselines.
- Identifying configuration items.
- Tracking and controlling changes.
- Establishing configuration management records
- Performing configuration audits.

POLICY:

DTMB and its client agencies are required to follow the process-based methodology for CM for all new initiatives as well as enhancement and maintenance of existing systems.

Agency Director:

- As a SOM Network and IT Customer, the Director within their area of responsibility shall ensure:
 - Financial compliance with Federal, State and regulatory laws governing the purchase of CI.
 - Maintaining ongoing legal compliance to meet all audit requirements for maintaining service assets.
 - Compliance with this policy.
 - Internal agency policies and procedures are implemented, maintained and enforced that compliment and comply with this policy.
 - Implementing more stringent internal policies than those developed by DTMB is done so in conjunction with DTMB.

DTMB Director:

- As a SOM Network and IT Owner, the Director shall ensure:
 - A process is defined to account for all the track-able IT assets and configurations within the SOM and its services.
 - A process is defined that maintains control over the evolution of a system.
 - A process is in place to ensure that when change to a CI is necessary, an implementation plan is developed which assures that all necessary steps and processes to implement the change have been thoroughly identified and documented.
 - A process is in place to ensure that all changes to CI are approved and communicated prior to implementation of a change.
 - Appropriate policies, standards and procedures are developed, implemented and maintained to ensure accurate configuration information.
 - A process is in place to assist agencies with the information they need to accommodate their financial and expenditure planning while adhering to legal obligations.
 - A mechanism is in place to maintain a current and comprehensive knowledge base of IT developments, trends and best practices. This mechanism should provide the Chief Technology Officer (CTO) with insights on how new technologies can be most effectively introduced into the current SOM environment.
 - The appropriate policies, standards and procedures are developed, implemented and maintained to ensure the confidentiality, integrity and availability of all SOM IT resources.

Terms and Definitions:

Agency	The principal department of state government as created by Executive Organization Act, P.A. 380 of 1965.
Configuration Items (CI)	Any component that needs to be managed in order to deliver an IT Service. Information about each CI is recorded in a Configuration Record within the Configuration Management System and is maintenance through its lifecycle by CM. CI's typically include IT services, hardware, software, buildings, people, and formal documentation such as process documentation and SLA's.

Configuration Management (CM)	The process responsible for maintaining information about CI's required to deliver an IT Service, including their relationships. This information is managed throughout the Lifecycle of the CI. CM is part of an overall Service Asset and Configuration Management Process.
Data Custodian	An individual or organization delegated by a data owner that has responsibility for maintenance and technological management of data and systems.
Data Owner	An individual or organization – usually a member of senior management of an organization – that is ultimately responsible for ensuring the protection and use of data.
Information Technology (IT) Resources	Includes, but is not limited to, devices, networks, data, software, hardware, email, system accounts, and facilities provided to conduct official state business.
Integrity	Guarding against improper information modification and/or destruction, ensuring information has not been altered by unauthorized people and the assurance that the information can be relied upon to be sufficiently accurate for its purpose. Integrity considers all possible causes of modification, including software and hardware failure, environmental events, and human intervention.
Trusted Partner/ Business Partner	A person (<i>i.e.</i> , vendor, contractor, 3rd party, etc.) or entity that has contracted with the SOM to perform a certain service or provide a certain product in exchange for valuable consideration, monetary, or goods and services.

Authority:

- This policy obtains its authority from:
 - Administrative Guide [Policy 1305 Enterprise Information Technology](#).
 - The [Administrative Guide to State Government](#).
 - DTMB [IT Technical Policies, Standards and Procedures](#), which can be found on the DTMB Intranet.

Enforcement:

- All enforcement for this policy shall be in compliance with the standards and procedures of Administrative Guide [Policy 1305 Enterprise Information Technology](#).

Developing Standards and Procedures for this Policy:

- All requirements for developing standards and procedures for this policy shall be in compliance with Administrative Guide [Policy 1305 Enterprise Information Technology](#).

Exceptions:

- All exception requests to this policy must be processed in compliance with Administrative Guide [Policy 1305 Enterprise Information Technology](#).

Effective Date:

- This policy will be effective upon signature of the Administrative Guide approval memo by the DTMB Director.
