

STATE OF ALABAMA

Information Technology Policy

POLICY 605-00: CONFIGURATION MANAGEMENT

Changes to the hardware, software, or firmware of a system can have a significant impact on the security of the system. A configuration management (CM) process reduces the risk that any changes made to a system may result in a compromise to the system or data confidentiality, integrity, or availability in that it provides a repeatable mechanism for effecting system modifications in a controlled environment.

OBJECTIVE:

Establish responsibilities for managing configuration changes to State of Alabama information systems which includes all computer and network systems owned by and/or administered by State agencies, all platforms (operating systems), all computer sizes (personal computers through mainframes), and all application systems (whether developed in-house or purchased from third parties).

SCOPE:

This policy applies to all Executive Branch agencies, boards, and commissions except those exempt under The Code of Alabama 1975 (Title 41 Chapter 4 Article 11).

RESPONSIBILITIES:

Agency Management, Information Technology Organization:

Organizations shall implement a configuration management process that ensures system changes are thoroughly evaluated and tested and approved by management prior to implementation.

Organizational CM roles and responsibilities include:

System Owner:

The system owner serves as the authority for all matters of CM for the system. The system owner is responsible for developing functional requirements and verifying that the requirements are implemented appropriately.

CM Manager:

The CM manager is responsible for day-to-day CM activities, including:

- Documenting and implementing organizational CM plans/procedures
- Managing change requests and coordinating implementation of changes
- Ensuring that proposed changes do not adversely affect agency systems or data
- Conducting impact analysis of changes
- Approving, denying, or deferring changes
- Notifying users of system changes
- Ensuring existence of a process for storing, retrieving, and distributing CM materials
- Ensuring that an audit trail of changes is documented and maintained

Configuration Control Board (CCB):

CM responsibilities of the CCB include:

- Discussing and resolving change requests that require additional funding or resources to implement

- Ensuring that change requests do not adversely affect any systems or services related to the system or associated systems, subsystems, and facilities
- Evaluating CM metric information on funding and other CM-related issues

Information Security Officer (ISO):

The agency ISO is responsible for addressing security concerns related to the CM program and for providing expertise and decision support to the CCB and CM Manager. The ISO also:

- Serves as the principal advisor to the authorizing official, system owner, and Chief Information Security Officer on all matters (technical and otherwise) involving the security of the information system(s) they are responsible for
- Assesses the security impact of system changes
- Plays an active role in developing and updating system security plans

System Users:

System users are responsible for reporting any new requirements or deficiencies that are identified in current versions of the system, software, or supporting documentation.

Developers, Testers, and System Administrators:

Developers, testers, and system administrators are responsible for coordinating and working with the CM Manager and ISO to identify, resolve, implement, and test approved system changes.

NOTE: An individual is not limited to a single role (e.g., an individual can be both the System Owner and the CM Manager); however, separation of duties shall be addressed to ensure that changes are implemented only after being tested and approved.

ADDITIONAL INFORMATION:

Information Technology Guideline 605G1: Configuration Management Process

http://cybersecurity.alabama.gov/documents/Guideline_605G1_CM_Process.pdf

Information Technology Dictionary

http://cybersecurity.alabama.gov/documents/IT_Dictionary.pdf

By Authority of Director, Information Services Division, Department of Finance

DOCUMENT HISTORY:

Version	Release Date	Comments
600-05	3/21/2008	Original document
605-00	6/16/2011	New number and format