

 Georgia Technology Authority	Georgia Technology Authority	
Title:	Operational Change Control	
PSG Number:	SS-08-026.01	Topical Area: Security
Document Type:	Standard	Pages: 2
Issue Date:	3/31/08	Effective Date: 3/31/08
POC for Changes:	GTA Office of Information Security	
Synopsis:	Establishes requirement for changes to operational systems be controlled and monitored.	

PURPOSE

The purpose of change management in an information security infrastructure is to manage the effects of changes or differences in configurations on an information system or network. Change management allows system owners to follow a standard process for changing a configuration item or its status and to manage changes in a predictable and controlled manner. It allows system owners to assess, identify, and minimize the risks to operations and security prior to implementation.

SCOPE; ENFORCEMENT; AUTHORITY; EXCEPTIONS

See Enterprise Information Security Charter (policy)

STANDARD

System owners shall develop, implement and enforce formal change management responsibilities and procedures to ensure strict control of all changes to operational information systems' computing and communications infrastructure (hardware, software, networks and applications) and ensure adequate consideration of the potential security impacts of changes to an information system or its surrounding environment.

Change management procedures shall be documented and include:

- Record of technical description, impact type, priority and outcome:
 - Emergency/Routine
 - Major/minor
 - High/low
 - Success/Failure-backout
- Formal approval of proposed changes
- Process for emergency, unplanned changes
- An assessment of the potential impact of changes

Title:	Operational Change Control
--------	----------------------------

- Testing changes prior to implementation
- Transferring software or hardware from development/test to production
- Communication of change details to all relevant persons
- Back-out procedure for aborting and recovering from unsuccessful changes

RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

- Change Management (Policy)

REFERENCES

- NIST SP800-100 Information Security Handbook for Managers (Ch 14)
- NIST SP 800-64 Security Consideration for SDLC
- NIST SP800-40 Procedures for Handling Security Patches

TERMS and DEFINITIONS

Change Management is the process of controlling modifications to hardware, software, firmware, and documentation to ensure that Information Resources are protected against improper modification before, during, and after system implementation.

Changes include:

- Any implementation of new functionality (including OS upgrades)
- Any interruption of service (scheduled or unscheduled)
- Any repair of existing functionality (including patch, virus and security updates)
- Any removal of existing functionality
- Maintenance routines
- Hardware installations/upgrades

Note: The PSG number was changed from S-08-026.01 on September 1, 2008

Effective Date:	March 31, 2008	2 of 2
-----------------	----------------	--------