
Topics:

[change \[2\]](#) **Change Management [1]**

PS-08-015 Change Management

Issue Date: 3/20/2008

Revision Effective Date: 3/20/2008

PURPOSE

Computer systems and the environments in which they operate change continually. Unauthorized changes in an operational system or environment create an unstable configuration baseline that can introduce vulnerabilities that could negatively impact the security posture of the information resource.

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 (including hardware, software and infrastructure). Change management allows system owners to handle changes in a controlled, predictable and repeatable manner and assess, identify and minimize the risks to operations and security prior to implementation.

POLICY

State of Georgia information systems, in the operations phase of the system lifecycle, shall have formal change control procedures that adequately consider the potential security impacts of the change to the information system or its surrounding environment.

System Owners shall establish formal change management procedures that include a process to document, review, approve, and monitor all changes to operational computing and communications infrastructure and assess the risks, impacts and benefits of the change.

RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

[Operational Change Control \(SS-08-026\)](#) [3]

REFERENCES

NIST SP 800-100 Information Security Handbook for Managers (Ch 14)

NIST SP 800-64 Security Consideration for SDLC

TERMS and DEFINITIONS

Change Management is the process of controlling modifications to hardware, software and infrastructure to ensure