IT0125 - Configuration Management

Objective:

To establish policy for a security-focused Configuration Management program to ensure compliance with minimally acceptable system configuration requirements.

Scope:

This policy applies to all users of and information technology (IT) resources owned, operated, or provided by the University of Tennessee System including its campuses, institutes, and administration (University and/or Campuses).

“Users” includes but is not limited to students, faculty, staff, contractors, agents, representatives, and visitors accessing, using, or handling the University’s information technology resources.

Information transmitted or stored on University IT resources is the property of the University unless it is specifically identified as the property of other parties.

Principles:

The University has chosen to adopt the policy principles established in the National Institute of Standards (NIST) 800 series of publications, and this policy is based on those guidelines.

The Chancellor or equivalent at each Campus must designate an individual or functional position responsible for information security at their Campus (Position of Authority and/or Campus Authority). The individual or position should be at a high enough organizational level to allow him/her/it to speak with authority on and for the Campus.

Each Campus must develop or adopt and adhere to a program which demonstrates compliance with this policy and related standards. This program is the responsibility of the Position of Authority.

A Campus may apply more stringent requirements than those documented in this policy provided they do not conflict with or lower the standards or requirements established by this or any other University policy.

Each User of University resources is required to be familiar and comply with University policies. Acceptance of this policy is assumed if a User accesses, uses, or handles University resources.

Policy:

Each of the University’s Campuses must develop or adopt and adhere to a formal, documented program that ensures the implementation of appropriate and effective system Configuration Management (CM) controls for business-critical systems designated and approved by the Position of Authority.

Mandatory Controls:

Mandatory security controls for business-critical systems are University-wide controls that are required to be consistently designed, implemented, and monitored, and assessed by all campuses:

1. **Baseline Configuration** (CM-2): Each Campus must develop, document, and maintain a record of baseline configurations for information systems.
   a. Baseline Configuration (CM-2 Enhancements):
      I. Review baseline configurations at least annually (CM-2.1).
      II. Retain a designated number of previous configurations to support audit and rollback (CM-2.3).
2. **Configuration Change Control** (CM-3): Each Campus must:

   a. Determine the types of changes to the information systems that are configuration-controlled;
   b. Review and approve/disapprove proposed changes;
   c. Document configuration change decisions;
   d. Implement approved changes to the information system;
   e. Retain records of changes;
   f. Review activities associated with changes to the information system; and
   g. Coordinate and provide oversight for configuration change control activities through a change control entity that convenes regularly.

3. **Security Impact Analysis** (CM-4): Changes to systems must be reviewed for their potential security impact prior to implementation.
4. **Least Functionality** (CM-7): Systems must be configured to provide only essential capabilities. Non-essential services, functions, ports, protocols, etc. should be disabled or restricted.
5. **Configuration Management Plan** (CM-9): Each Campus must develop or adopt and implement a configuration management plan that:
   a. Addresses roles, responsibilities, and configuration management processes and procedures;
   b. Establishes a process for identifying and managing system configurations throughout the system development life cycle, and placing systems under configuration management; and
   c. Protects the configuration management plan from unauthorized disclosure and modification.

Discretionary Controls:

Discretionary Controls are security controls whose scope is limited to a specific campus, institution, or other designated organizational component. Discretionary Controls are designed, implemented, monitored, and assessed within that organizational component. Discretionary controls must not conflict with or lower the standards established by Mandatory Controls.

References:

1. NIST 800-53 *"Recommended Security Controls for Federal Information Systems and Organizations"*

Definitions:

1. **Configuration Management** - comprises a collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems.
2. A **Baseline Configuration** - is a set of specifications for a system, or Configuration Item (CI) within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The Baseline Configuration is used as a basis for future builds, releases, and/or changes.
3. **Configuration Change Control** - is a process for managing changes to the Baseline Configurations for Configuration items.
4. **Position of Authority** - is that person, as designated by the Chancellor, who is responsible for information security at their Campus

Last Reviewed: January 11, 2017