

BSD & UCM Cyber Security Policy Summary

Policy Name: Configuration Management Policy

Date: December 11, 2015

Purpose

The **Configuration Management Policy** sets requirements for maintaining system inventory and defines the process for managing configuration changes to mission critical systems through a formal review process.

Policy Summary

Definitions

- **Protected Information** - Information that needs to be protected, as mandated by laws or regulations (e.g. Patient records, Social Security Numbers etc.).
- **Covered Individuals** - Employees and students of UCMC and BSD (e.g. Administrators, Faculty, Staff and Users) including third parties with access to the Organizations' Information Systems.
- **Information System Owners** - Employees of the Organization who are Director level, faculty, or above and has the ultimate responsibility over a particular Information System.
- **Departmental and Unit Leaders** - Department Chairs, Section Chiefs, Executive Directors, Directors, Managers, Supervisors, etc.
- **Information System** - Server based software that resides on a server or multiple servers used for business purposes. "Application" or "Information System" is synonymous with "System". E.g. A database server, web server or other application server.

General Summary

- Information System Owners must establish technical procedures that align to the risk based controls defined within the policy.
- Information System Owners must maintain an inventory of IT equipment in accordance to standards and procedures.
- IT Custodians must implement configuration baselines for IT equipment under their technical support.
- Users that manage their own IT equipment for work related activities must register the equipment with the applicable Information Security Office.
- Configuration changes to Information Systems must be reviewed through a change control process that includes a review of potential security issues prior to implementation.
- IT Custodians must limit the use of software to licensed purposes only, in accordance with copyright laws.
- A summary of the responsibilities outlined in the policy are provided in the table below.

Roles	Administrators Faculty, Staff and Users	Information System Owners and IT Staff	Executive Management
Responsibilities			
Maintain an inventory of IT equipment		✓	
Establish and implement configuration baselines		✓	
Review configuration changes to Information Systems		✓	
Limit the use of software to licensed purposes only		✓	