BSD & UCM Cyber Security Policy Summary
Policy Name: Audit and Accountability Policy
Date: December 11, 2015

Purpose

The **Audit and Accountability Policy** defines the methods for managing user access audit records to enable the monitoring, analysis and investigation of inappropriate information system activity.

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 Systems with Protected Information must be setup with automatic logging and alerting mechanisms.
- Information Systems with Protected Information must maintain audit logs for a period no less than 3 months.
- Automatic alerting mechanism must be setup to notify IT Custodians when unusual or malicious activities are encountered.
- Unusual or malicious activities must be investigated by an IT Custodian and reported to the applicable Information Security Office.
- 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			
Establish technical procedures		✓	
Setup automatic logging and alerting mechanisms.		✓	
Maintain audit logs for at least 3 months.		✓	
Investigate and report unusual or malicious activities		✓	