BSD & UCM Cyber Security Policy Summary
Policy Name: Access Control Policy
Date: September 14, 2015

Purpose

The **Access Control Policy** defines the methods for how users will be provided access to Information Systems, such as EPIC, Centricity, Redcap and Oracle. Additionally, it defines the rules relating to how often access management should be reviewed, how to determine a user's privileges, and when to remove access. The target audience of the policy is geared towards Information System Owners and IT Custodians.

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.).
- **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.
- **Covered Individuals** - Employees and students at UCMC and BSD (e.g. Administrators, Faculty, Staff and Users) including third parties with access to the Organizations' Information Systems.
- **Departmental and Unit Leaders** - Department Chairs, Section Chiefs, Executive Directors, Directors, Managers, Supervisors, etc.
- **Information System Owners** - Employees of the Organization, Director level or above who have the ultimate responsibility over a particular Information System.
- **Information Owner** - Employees of the Organization who are Director level, faculty, or above, responsible for classifying Information and ensuring access to the information is appropriate.

General Summary

- Information Owners are responsible for determining which groups or populations of individuals are able to access the Information they are responsible for, and Information Systems the Information may reside.
- Information System Owners are ultimately responsible for ensuring the access controls are consistent with the expectations of the Information Owner and that their users are accessing their systems in accordance with this policy.
- IT staff are responsible for developing and executing the technical procedures for access management.
- Technical procedures must be developed which align to the risk based controls defined within the policy.

Roles Responsibilities	Administrators Faculty, Staff and Users	Information System Owners and IT Staff	Information Owner
Determining who is permitted to access Information			✓
Set technical access controls to Information and Systems		✓	
Access systems in accordance to policy	✓		