BSD & UCM Cyber Security Policy Summary
Policy Name: Responsibilities and Oversight Policy
Date: September 14, 2015

Purpose

The **Responsibilities and Oversight Policy** explains the different types of roles and responsibilities of management, administrators, faculty and staff for safeguarding information systems and information (e.g. Protect Health Information, private research data etc.) This policy also serves as the foundation for subsequent cyber security policies.

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.
- **Executive Management** - Dean of the Biological Sciences Division, the President of The University of Chicago Medical Center, Associate Dean's, Assistant Dean's, Vice Presidents, and Research Executives.

General Summary

- The BSD and UCM Chief Information Security Officers have been mandated to defend their organizations against cyber threats. This is done through identifying, monitoring, and responding to cyber threats and vulnerabilities and implementing controls to manage risk.
- Everyone has a part in safeguarding Protected Information, whether they have direct responsibility for determining its safeguards, or are serving as guardians of the information received from others.
- A summary of the roles and responsibilities outlined in the policy are provided in the table below.

Roles Responsibilities	Administrators Faculty, Staff and Users	Information System Owners and IT Staff	Departmental and Unit Leaders	Executive Management
Safeguard Protected Information	✓	✓	✓	✓
File an exceptions when cannot meet policy	✓	✓		
Respond to corrective actions related to cyber risks		✓	✓	✓
Ensure employees complete security awareness training			✓	
Own cyber risk decisions for the organization				✓