BSD & UCM Cyber Security Policy Summary

Policy Name: Physical and Environmental Protection Policy
Date: December 11, 2015

Purpose

The **Physical and Environmental Protection Policy** defines the physical controls that must be in place to protect Information Systems from physical unauthorized access and safeguard against environmental threats (e.g. power failures, etc.).

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 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.
- **Designated Secure Computing Facility –** Data center, server room or a closest built with the necessary physical security and environment (e.g. cameras, HVAC, redundant power etc.) required for servers.

General Summary

- Information Systems must be housed in a Designated Secure Computing Facility (DSCF) that meet the risk based controls outlined in this policy.
- Department and Unit Leaders providing physical space for Information Systems are responsible for implementing physical security controls in accordance risk based controls outlined in this policy.
- Information Systems in closets or rooms that do not meet the policy risk based controls must be relocated to the CBIS or University ITS data center with 1 year.
- Computer screens and displays in public areas used for showing Protect Information must be setup to limit the view of curious onlookers.
- Electronic devices in public areas must be secured with a security cable lock to prevent theft.
- 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			
House Information Systems in Designated Security Computing Facilities		✓	
Limit the view on displays that show Protected Information in public areas		✓	
Secure electronic devices in public areas with a security cable locks	✓	✓	