

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	October 2004
Section 5.8	Information Security	Revised:	May 2011
Policy 5.8.24	Change Management Security Policy	Responsibility:	Chief Information Security Officer

CHANGE MANAGEMENT SECURITY POLICY

Overview

This document establishes a “Change Management Program” at the Health Science Center. A structured change process can minimize vulnerabilities of information resources, limit their exposure to exploitation and attack, and maximize the protection available to prevent damage to the University.

Policy

1. To ensure reliable and stable operations, all departments managing information resources (examples: network infrastructure, desktop computers, decentralized servers, internal and outsourced applications, etc.) are required to establish best practice change management procedures and require compliance from individuals who manage such information systems and/or applications.
 2. All system changes (hardware, software, configuration, and application programming) require prior approval by the appropriate Dean, Chair, Director, or designee.
 3. Based on risk, each department should formalize change management procedures considering the following:
 - A mechanism to request and schedule a system change.
 - A mechanism to authorize a scheduled system change.
 - A mechanism for processing emergency system changes.
 - A log to document the proposal, approval, implementation, and review of system changes.
 - A change notification and coordination process for management and impacted users.
-