Configuration Management Policy

Policy 9	POL-CM	Effective Date	12/17/15	Review Date	12/17/15	Version	1.0

Table of Contents

I. PURPOSE

The University of Chicago Medical Center and the Biological Sciences Division of The University of Chicago (the "**Organizations**") protects information that is the subject of legal, contractual, or enterprise confidentiality and security requirements (collectively the "**Security Obligations**"); such information is called "**Protected Information**." This policy ensures the Organizations' Information Assets are managed in a secure manner, and that the information stored, transmitted or processed are protected and secure.

II. SCOPE

This policy applies to Information Assets (workstations, laptops, mobile devices, servers, software applications, enterprise applications, etc) that are owned by the Organizations. All Covered Individuals are subject to this policy.

Information Assets not owned by the Organizations (e.g. personally owned devices, third parties) are subject to different requirements.

III. POLICY

Each CISO will define Standards to (i) establish and maintain security baseline configurations (ii) ensure inventories of Organizational Information Assets (including hardware, software, firmware, and documentation) are managed and maintained throughout the respective Information Asset life cycles, and (iii) process to manage changes to the Information Assets.

Capitalized terms used in this policy are defined in the glossary attached. The CISOs together may change the definitions in the glossary without the approval of the Executive Cyber Risk Committee.

IV. PROCEDURES

1. Information System Owners must maintain and document technical procedures that meet the Risk Controls set forth below and comply with Standards. IT Custodians must implement the documented technical procedures that meet the Risk Controls set forth below. Information System Owners and IT Custodians may seek guidance from the CISOs in developing technical procedures.

2. Information System Owners are responsible for maintaining an inventory of Endpoints and Information Systems managed within their purview. The inventory must be produced by the Information System Owner to either CISO of either Organization upon reasonable request. At a minimum, the inventory must include the following information:

    a. Hostname
    b. MAC address (wired)
    c. MAC address (wireless)
    d. Primary User (or appropriate designation if the asset is shared)
    e. Owning Organization (BSD, UCMC or UChicago)
    f. Supervisory Organization ID (e.g department Cost Center)
    g. Operating System (the OS with service pack level)
    h. Device Type (server, workstation, laptop, mobile device)

3. Covered Individuals who manage their own Endpoints and Information Systems without support from an IT services group must register and maintain their Endpoints and Information Systems in accordance to the respective Information Security Office's standards and procedures. As general guidance, Covered Individuals within the clinical functions of the Organizations will register their devices with the UCM Information Security Office; Covered Individuals within the research and academic functions of the Organizations will register their devices with the BSD Information Security Office.

4. Information System Owners are responsible for ensuring changes to their Information Systems have been documented and reviewed through a change control process. The change control process must be approved by the respective CISO.

5. It is the responsibilities of the Information System Owners to retain all the documents referenced above.

The Organizations will use the Risk Based Controls below to implement the procedures.

V. RISK BASED CONTROLS

Risk based controls are organized in three categories; Core (C), Low (L) and Moderate (M). Core controls are mandatory for all Information Systems. Information Systems designated as FISMA Low must comply with Low controls, in addition to the Core controls. Information Systems designated as FISMA Moderate must comply with Moderate controls, in addition to the Low and Core controls.

Baseline Configuration (CM-2 CM)

Core	Technical procedures must be developed, documented and maintained which define the baseline configurations for their Information Assets (endpoints, servers, etc). These baselines will be managed leveraging versioning and configuration control.
Low	N/A
Moderate	• Review and update the baseline configurations of Endpoint and Information Systems on a periodic basis and as an integral part of Information System component installations and upgrades. • Retain at least one (1) previous version of baseline configurations to support rollbacks, if necessary. • As required by the respective CISO of the Organizations, Endpoints with a higher baseline security standard to Covered Individuals will be used when traveling to countries of significant risk and apply additional sanitization safeguards to those Endpoints when the Covered Individuals return.

Configuration Change Control (CM-3 CM)

Core	Changes to baseline configurations of Endpoints and Information Systems will be managed in accordance with applicable change management procedures.
Low	N/A

Moderate	• Changes must be tested, validated and documented before making the change to any Information Asset. The procedures should include, at a minimum:
	  ○ The change request process with related forms and work flow
	  ○ Test plan requirements
	  ○ Emergency change procedures
	• Change requests must be reviewed and approved by the appropriate Information System Owner, or other Departmental or Unit Leader, prior to

	the change being authorized. • Emergency changes to an Information Asset must be documented and approved by an Emergency Change Advisory Board. All emergency changes must be reviewed post change by the CAB. • Documentation of change control must be kept for a period of six (6) years by the applicable IT Custodian

Security Impact Analysis (CM-4 CL)

Core	Changes to Information Assets will be analyzed to determine potential security impacts prior to change implementation. This analysis can occur through the normal and regular CAB meetings.
Low	Authorized security personnel conduct security impact analyses, which should include, but not limited to, risk analysis, reviewing security plans to understand security control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls.
Moderate	N/A

Access Restrictions for Change (CM-5 M)

Core	N/A
Low	N/A
Moderate	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the Information System, including at a minimum: • Limit to specific roles the privilege to change Information System components and system-related information within a production or operational environment • Limit privileges to change software resident within software libraries • Review and reevaluate change privileges on a periodic basis

Configuration Settings (CM-6 CL)

Core	• Configuration settings must be established, documented and implemented that are specific to the Information Asset that reflect the most restrictive operational mode possible while maintaining operational requirements. •
Low	• Deviations from baseline configuration settings must be approved by the respective CISO of the Organizations. • Changes to configuration settings must be submitted, and approved, through the change control procedures.
Moderate	N/A

Least Functionality (CM-7 CM)

Core	• Information Assets must be configured to provide only essential capabilities. The functions and services provided by Information Assets must be reviewed carefully to determine which functions and services are candidates for elimination or restriction (e.g., File Transfer Protocol [FTP], Hyper Text Transfer Protocol [HTTP] etc.). • The use of those non-essential functions, ports, protocols, and/or services must be prohibited and/or restricted.
Low	N/A
Moderate	• Information Assets shall be reviewed on a periodic basis to identify unnecessary and/or nonsecure functions, ports, protocols, and services. Functions, ports, protocols, and services within the Information Asset deemed to be unnecessary and/or nonsecure shall be disabled. • Approved software programs will be managed and inventoried and Information Assets will be configured to prevent execution of unauthorized software execution. This shall be done through an allow-all or deny-by-exception policy. • Approved software programs will be reviewed and updated on a periodic basis.

Information System Component Inventory (CM-8 LM)

Core	Procedures must be developed to document and maintain a current inventory of Information Assets and relevant ownership information, as defined within the Procedures section of this policy. Inventory shall be reviewed and updated as need/required.
Low	N/A
Moderate	• Inventories lists will be managed as part of regular Information Asset maintenance • Management of Information Assets will be conducted through automated mechanisms which will, at a minimum: o Detect presence of unauthorized software, hardware and firmware components o Update Information Asset ownership information to be current o Automatically enforce restrictions on the Information Asset if unauthorized components are detected • Information Asset components will be verified within its authorization boundary of the Information System to ensure it is not duplicated in other Information System component inventories.

Configuration Management Plan (CM-9 M)

Core	N/A
Low	N/A
Moderate	A Configuration Management Plan must be developed, documented and

	maintained that: • Addresses the roles, responsibilities, and configuration management processes and procedures. • Establishes a process for identifying configuration items throughout the system development life cycle (SDLC) and management of the configuration of the configuration items. • Defines the configuration items for the Information Assets and place the configuration items under configuration management. • Protects the configuration management plan from unauthorized disclosure and modification.

Software Use Restrictions (CM-10 CL)

Core	Procedures must be developed, documented, and implemented effectively to limit the use of software for only licensed purposes and according to contract agreements and copyright laws.
Low	• Software licenses, and associated documentation, will be tracked by quantity of licenses to control the copying and distribution • Use of peer-to-peer file sharing technologies will be controlled to ensure this capability is not used for unauthorized distribution, display, performance or reproduction of copyrighted work.
Moderate	N/A

User Installed Software (CM-11 L)

Core	N/A
Low	Information Assets will be configured in a manner that: • Prohibits the installation of software by users. • Enforces software installation through central management methods • Is monitored for compliance with these restrictions on a periodic basis
Moderate	N/A

VI. Cross References

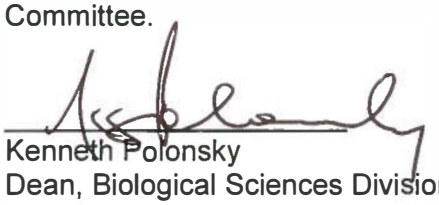
POL-RO Responsibility and Oversight Policy
POL-AC Access Control Policy
POL-BD Personally Owned Computing Devices Policy

VII. Policy References

HIPAA Security Rules: 42 C.F.R. § 164.308(a)(1)(i).

VIII. INTERPRETATION, IMPLEMENTATION AND REVISION

Each CISO is responsible for the interpretation and implementation of this policy, and responsible for recommending revisions of this policy to the Cyber Security Executive Committee.



Kenneth Polonsky
Dean, Biological Sciences Division

Sharon O'Keefe
President, The University of Chicago Medical Center

IX. Approval and Ownership

Owner	Title	Date
Privacy & Security Steering Committee	Policy Development Group	12/11/15
Approved By	**Title**	**Date**
Kenneth Polonsky, MD	Richard T. Crane Distinguished Service Professor, Dean and EVP for Medical Affairs	12/17/15
Sharon O'Keefe, RN	President, University of Chicago Medical Center	12/17/15

X. Revision History

Version	Description	Review Date
1.0	Initial Version	8/4/15