

# Risk Assessment and Management Policy

Policy 13	POL-RM	Effective Date	8/8/17	Review Date	8/8/17	Version	1.0
-----------	--------	----------------	--------	-------------	--------	---------	-----

## Table of Contents

I.	Purpose .....	1
II.	Scope.....	1
III.	Policy .....	2
IV.	Procedures .....	2
V.	Risk Based Controls.....	4
	Risk Assessment Policy and Procedures (RA-1 C) .....	4
	Security Categorization (RA-2 CL) .....	4
	Risk Assessment (RA-3 C).....	4
	Vulnerability Scanning (RA-5 CM).....	4
	Plan of Action and Milestones Process (PM-4 C) .....	5
	Risk Management Strategy (PM-9 C) .....	5
VI.	Cross References.....	6
VII.	Policy References .....	6
VIII.	Interpretation, Implementation and Revision .....	6
IX.	Approval and Ownership.....	7
X.	Revision History .....	7

## I. PURPOSE

The University of Chicago Medical Center and the Biological Sciences Division of The University of Chicago (the “**Organizations**”) protect 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 that the Organizations conduct risk assessments to organizational operations, assets, and individuals resulting from the operation of Organizations’ Information Systems and its associated processing, storage or transmission of the Organizations’ information. This policy also ensures that identified risks are managed according to the Organizations’ expectations.

## II. SCOPE

This policy applies to the Organizations’ (i) Covered Individuals, (ii) Information Systems and Endpoints, (iii) the Organizations’ electronic information and (iv) the business processes run by Covered Individuals leveraging the Organizations’ Information Systems, Endpoints and electronic information.

### III. POLICY

The Organizations must periodically assess, identify and prioritize the potential cybersecurity risks and vulnerabilities to the confidentiality, integrity and availability of organizational operations, Information Systems and Endpoints, and Covered Individuals.

Cybersecurity risks (herein referred to as “risks”) that have been identified by the Organizations are evaluated by the likelihood of threats exploiting vulnerabilities, and their impact to the Organizations. Once evaluated, risks will be managed by the Organizations through a series of risk management techniques that reduces the level of risk to the Organizations to a level deemed acceptable by the Executive Managers.

Capitalized terms used in this policy are defined in the POL-RO Responsibilities and Oversight Policy. The CISOs together may change the definitions in the glossary without the approval of the Executive Cyber Risk Committee.

### IV. PROCEDURES

1. The CISOs of the Organizations must maintain and document technical and administrative processes and procedures that meet the risk based controls set forth below.
2. The CISOs of the Organizations ensure the BSD and UCMC apply consistent risk ranking mechanisms.
3. The CISOs of the Organizations periodically conduct risk assessments, using the threat, vulnerability, and impact methodologies, of Information Systems and Endpoints, business processes, third party relationships or affiliations, and information practices.
4. Upon determination of any risks, the CISOs produce a remediation action plan which is designed to reduce the risk down to an acceptable level of tolerance as determined by Executive Management. The CISOs and Executive Management, Departmental or Unit Leaders, or System Owners will review and finalize the recommended remediation action plan. This remediation action plan can leverage one or more of the following risk management strategies:
  - a. Remove the risk entirely by decommissioning affected component that has actualized the risk
  - b. Reduce the risk to an acceptable level, as determined by the Executive Managers, by implementing additional controls
  - c. Transfer the responsibility to a third party (non-Organizational entity) and ensuring the risk is appropriately managed through such transfer
  - d. Acceptance of the risk in its current state by the appropriate Executive Manager
5. On an annual basis, the CISOs of the Organizations will
  - a. Update the assessment of the current enterprise cyber risk posture
  - b. Conduct a risk assessment of the Certified EHR to meet the Center for Medicaid and Medicare (CMS) Meaningful Use requirements and objectives.

6. To continually assess and manage ongoing risk to the Organizations, Departmental and Unit Leaders, Information System Owners and IT Custodians must notify the respective CISO of the Organizations under the following circumstances:
  - a. Department and Unit Leaders
    - i. When new Information Systems are introduced into the Organizations
    - ii. When introducing new or updated business processes which includes significant uses of information with third parties
    - iii. When significant changes occur to their Information Systems
  - b. Information System Owners and IT Custodians:
    - i. When discovering cyber risks during the course of their duties
    - ii. When introducing significant new Information Systems into the Organizations
    - iii. When significant changes occur to their Information Systems

The CISOs, or their delegates, will evaluate the reported risk pursuant to this policy.

7. Risks that have been identified pursuant to the procedures in this policy will be logged within the Organizations' risk registers by the CISOs, or their delegates.
8. Executive Managers, Departmental and Unit Leaders, System Owners and IT Custodians will cooperate with the CISOs on risk assessment. Their obligations are as follows:
  - a. Executive Managers:
    - i. Support the Organizations' ongoing risk assessment and management processes
    - ii. Address or accept identified cyber risks
  - b. Departmental and Unit Leaders:
    - i. Provide resources to facilitate risk assessments and risk management activities
    - ii. Manage risks identified within their departments or units, according to the identified remediation plans
  - c. Information System Owners:
    - i. Support risk assessments and provide any documentation necessary
    - ii. Determine the final remediation plan, in collaboration with the CISOs (or their delegates)
    - iii. Implement remediation plans that were identified as part of the risk assessment activities,
    - iv. Report the status of said activities to the respective CISOs of the Organizations
  - d. IT Custodians:
    - i. Provide the documentation necessary for conducting risk assessment activities
    - ii. Implement the controls that were identified as part of the remediation plans
9. Any records and compliance reports pertinent to compliance with federal and state laws, such as risk assessments, and actions and activities that the HIPAA Security Standards require to be documented, will be kept for a period of six (6) years.

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.

### Risk Assessment Policy and Procedures (RA-1 C)

<b>Core</b>	The CISO of each Organization defines, documents and disseminates a risk assessment policy and procedure that ensures Organizational cyber risks are controlled at an acceptable level.
<b>Low</b>	N/A
<b>Moderate</b>	N/A

### Security Categorization (RA-2 CL)

<b>Core</b>	Categorization and document the Information and Information System according to Confidentiality, Integrity and Availability requirements.
<b>Low</b>	<ul style="list-style-type: none"> <li>Document the results of the security categorization within the security plan for the Information System</li> <li>Ensure that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision</li> </ul>
<b>Moderate</b>	N/A

### Risk Assessment (RA-3 C)

<b>Core</b>	<p>Risk assessments are conducted, including the likelihood and impact, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the Information System, the information it stores, processes and transmits</p> <p>Results of the risk assessments are delivered to the appropriate Executive Manager, Departmental or Unit Leader, and/or System owner and documented in the Organizations risk register.</p> <p>The risk assessments will be updated periodically, or upon determination by the appropriate CISO based upon a significant change to the Information System or environment.</p>
<b>Low</b>	N/A
<b>Moderate</b>	N/A

### Vulnerability Scanning (RA-5 CM)

<b>Core</b>	<p>The Organizations' Information Security Offices:</p> <ul style="list-style-type: none"> <li>• Scan for vulnerabilities within Information Systems on monthly basis at a minimum</li> <li>• Use vulnerability management tools that can automate the vulnerability management process by: <ul style="list-style-type: none"> <li>○ Enumerating the Information Assets platforms, software flaws and configurations</li> <li>○ Measuring the vulnerability's impact</li> </ul> </li> <li>• Analyze the results of vulnerability scans and ensure that vulnerabilities are remediated by the applicable System Owner or IT Custodian in accordance with its level of risk or a standard</li> </ul>
<b>Low</b>	N/A
<b>Moderate</b>	<p>The Organizations' Information Security Offices:</p> <ul style="list-style-type: none"> <li>• Deploy vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned</li> <li>• Use authenticated scanning to check Information Systems configuration settings compared against checklists and test procedures</li> <li>• Implement authenticated vulnerability scanning of Information Systems with Protected Information to ensure the accuracy of the scans while minimizing impact</li> <li>• Share information obtained from vulnerability scanning with Departmental or Unit Leaders and System Owners to help eliminate similar vulnerabilities in other Information Systems</li> </ul>

**Plan of Action and Milestones Process (PM-4 C)**

<b>Core</b>	<p>The Organizations' Information Security Offices will ensure that appropriate remediation action plans are developed, documented and disseminated based upon the results of the applicable risk assessment. This documentation will be kept for a period of six (6) years. The plans will document the remedial information security actions to adequately respond to risk to the Organizations' operations, Information Systems, business processes and Covered Individuals.</p>
<b>Low</b>	N/A
<b>Moderate</b>	N/A

**Risk Management Strategy (PM-9 C)**

<b>Core</b>	<p>The Organizations' Information Security Offices:</p> <ul style="list-style-type: none"> <li>• Develop a comprehensive strategy to manage cyber risk to the Organizations' operations, Information Systems, business processes, and Covered Individuals</li> <li>• Implement the risk management strategy consistently across the organization</li> </ul>
-------------	---

	<ul style="list-style-type: none"> <li>Review and updates the risk management strategy on a routine basis, or as required, to address organizational changes.</li> </ul>
<b>Low</b>	N/A
<b>Moderate</b>	N/A

## **VI. CROSS REFERENCES**

POL-RO Responsibility and Oversight Policy

## **VII. POLICY REFERENCES**

HIPAA Security Rules: 42 C.F.R §164.308 (a)(1)(i), (ii)(A),(B),(E),(iii) and 42 C.F.R §164.316 (b)(2)(iii)

## **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 Executive Cyber Risk 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	4/20/17
Approved By	Title	Date
Kenneth Polonsky, MD	Richard T. Crane Distinguished Service Professor, Dean and EVP for Medical Affairs	8/8/17
Sharon O'Keefe, RN	President, University of Chicago Medical Center	8/8/17

## X. REVISION HISTORY

Version	Description	Review Date
1.0	Initial Version	8/8/17