System and Service Acquisition Policy

Policy 10	POL-SA	Effective Date	MM/DD/YYYY	Review Date	MM/DD/YYY	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 sufficient protection of Information Assets or technology services during the acquisition of assets or services. This is accomplished by setting procedures with regard to life-cycle management and resource allocation.

II. SCOPE

This policy applies to Covered Individuals who acquire the Information Assets or technology services on behalf of the Organizations, as well as the Information System Owners and IT Custodians responsible for managing and maintaining Information Assets.

III. POLICY

This policy defines methods that must exist in order for the Organizations to (i) confirm the allocation of sufficient resources to adequately protect organizational Information Assets, (ii) set guidelines on the adoption and operation of Information System development life cycle processes that incorporate information security, such as software usage and installation restrictions, and (iii) when necessary, evaluate third-party providers for adequate security measures to protect information, applications, and/or services outsourced from the Organizations.

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. University Procurement or UCM Supply Chain, with the appropriate CISO of the Organizations, will agree and implement procedures that address security needs when executing contracts related to Information Systems or technology services.

    a. The UCM CISO will be responsible for the following Information Asset or technology service acquisitions: All UCMC operations, clinical trials and clinical operations of the BSD.

    b. The BSD CISO will be responsible for the following Information Asset or technology service acquisitions: BSD research, education and administrative operations.

2. Contracts will contain a Security Standards Addendum (SSA), security terms and standards as an addendum to the contract, managed and approved by the CISOs of the Organizations. Changes to an SSA may only be approved by the appropriate CISO of the Organization, in consultation with the respective Office of Legal Affairs.

    The appropriate CISO of the Organizations, or their delegate, will execute the appropriate third-party risk management process, when appropriate, on third party vendors, inclusive of vendors that are defined as Business Associates under HIPAA, to identify material risks to inform the acquisition process accordingly.

3. The Executive Management of the Organizations will allocate dedicated Information Security budgets proposed by the CISOs of the Organizations.

4. Covered Individuals who acquire Information Assets (Equipment Coordinators) will follow the Information Asset procurement standards and procedures set forth by the CISO of each Organization.

5. Equipment Coordinators will ensure technology, as categorized below, are delivered to the appropriate IT Custodians to be readied for operation and inventoried prior to use by Covered Individuals:
    a. Acquisition of Endpoints for the use by Covered Individuals

b. Acquisition of Information Systems for deployment within the Organizations network/environment; and
c. Acquisition of Cloud based services (e.g. SaaS) for use within departments

6. IT Custodians will ensure the applicable Information Security policies, procedures and standards are met prior to deployment into the production environment and use by Covered Individuals.

7. Department Head and Unit Leaders are accountable for monitoring of noncompliance with the assets procurement standards and procedures.

8. Information System Owners and IT Custodians will develop, document and implement the proper security standards based upon the classification of the Information Asset. The CISOs of the Organization may periodically review this documentation for conformity to the Organizations policies and procedures. Security standards documentation will be kept by the Information System Owner for a period of six (6) years.

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

V. RISK BASED CONTROLS

System and Services Acquisition Policy and Procedures (SA-1 C)

Core	The CISO of each Organization establishes controls and procedures for the acquisition of Information Assets and technology services while Covered Individuals who are acquiring Information Assets and technology services follow the Organizational procedures set to ensure their protection and security. Departmental and Unit Leaders ensure that Covered Individuals under their supervision abide by the policies and procedures created by the CISOs and Information System Owners.
Low	N/A
Moderate	N/A

Allocation of Resources (SA-2 C)

Core	• Determine security requirements for Information Assets or technology services during business process planning • Determine, document and allocate resources required to protect the Information Asset or technology service as part of the capital planning control development processes • Establish a discrete budget for the Organizations' CISOs and their security programs, as well as budgets appropriate for establishing security controls for Information Assets or technology services
Low	N/A
Moderate	N/A

System Development Life Cycle (SA-3 C)

Core	• System Development Life Cycle frameworks and processes used within the Organizations incorporate information security considerations • Information Security roles and responsibilities are documented throughout the SDLC process, including the setting responsibilities to IT Custodians of Information Assets for information security • Organizational risk management processes are integrated into the established SDLC
Low	N/A
Moderate	N/A

Acquisition Process (SA-4 C)

Core	As part of the acquisition of Information Assets or technology services will be acquired through defined procedures. Additionally, acquisition contracts will account for security functional requirements, security strength requirements, security assurance requirements, security-related documentation requirements, requirements for protecting security-related documentation, a description of the environment the Information Asset or technology service is intended to operate, and acceptance criteria.
Low	N/A
Moderate	N/A

Information System Documentation (SA-5 C)

Core	• Administrative documentation of the Information Asset or technology service will contain the following:
	  ○ Secure configurations, installation and operation
	  ○ Effective use and maintenance of security functions
	  ○ Known vulnerabilities regarding configuration and use of administrative functions
	• User documentation of the Information Asset or technology service will contain the following:
	  ○ User-accessible security functions and how to effective use those security functions
	  ○ Methods for user interaction, which enables individuals to use the system in a more secure manner
	  ○ User responsibilities in maintaining the security of the system
	• Documentation will be protected, available and distributed to the proper and appropriate Covered Individuals

Low	N/A
Moderate	N/A

Security Engineering Principles (SA-8 M)

Core	N/A
Low	Security engineering principles will be applied in specification, design, development, implementation and modification of the Information Asset or technology service.
Moderate	N/A

External Information System Services (SA-9 C)

Core	Third party vendors are required to comply with the Organizations information security requirement, and will be evaluated as part of the Organizations third party risk assessment procedures.
Low	N/A
Moderate	N/A

Developer Configuration Management (SA-10 M)

Core	N/A
Low	Information System Owners and IT Custodians will: • Perform configuration management • Document, manage and control integrity of changes to system configuration items • Implement only organizationally approved changes to the system • Document approved changes to the system and the potential security impacts of the change Track security vulnerabilities and vulnerability resolution of the system
Moderate	N/A

Developer Security Testing and Evaluation (SA-11 M)

Core	N/A
Low	Information System Owners and IT Custodians will: • Create and implement security assessment plans • Perform security testing prior to deployment to production environments • Provide evidence of execution of the security assessment plan and results of security testing • Implement flaw remediation processes • Correct flaws identified as part of the security testing process
Moderate	N/A

VI. CROSS REFERENCES

1. Department of Medicine Procurement Policy
2. UCMC: A01-02, Signature Authorization (defining purchasing levels)

3. UCMC: A01-03, Authority to Enter Into Contracts (who can sign)
4. UCMC: A01-06, Purchasing (only UCMC can buy for UCMC, conflicts of interest eval, MWSE tracking, only can purchase via Supply Chain and PO, RFP)
5. UCMC: A01-04, Capital Assets (rules around how to how to capitalize)

UChicago: Policy of Procurement and Engagement of Services

POL-CM: Configuration Management Policy

VII. POLICY REFERENCES

Insert the references—include both HIPAA security rule citations as well as NIST citations. The HIPAA security rule citations take the following format:
HIPAA Security Rules: 42 C.F.R. § 164.___(_)(_).

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	
Approved By	**Title**	**Date**
Kenneth Polonsky, MD	Richard T. Crane Distinguished Service Professor, Dean and EVP for Medical Affairs	
Sharon O'Keefe, RN	President, University of Chicago Medical Center	

X. REVISION HISTORY

Version	Description	Review Date
1.0	Initial Version	
2.0	Plamen, Marilyn & Erik	
3.0	Marilyn	