Physical and Environmental Protection Policy

Policy 7	POL-PE	Effective Date	12/17/15	Modified 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 defines the requirements for the physical, environmental controls and facility access controls to ensure the protection of Information Assets and Information Systems from unauthorized access and safeguard against environmental threats.

II. SCOPE

This policy applies to Designated Secure Computing Facilities (e.g. data centers, server rooms, data closets, etc.) and some parts apply to Information Assets (e.g. workstations) within public

areas accessible to non-Covered Individuals (e.g. waiting area, lobby, train etc.). All Covered Individuals are subject to this policy.

III. POLICY

This policy defines the physical and environmental controls that must exist to protect Information Assets and Information Systems from unauthorized access and safeguard against environmental threats. The Organizations require that (i) its facility and equipment are safeguarded from unauthorized physical access, tampering and theft by allowing access to only those who are entitled to have physical access to Information Assets and Information Systems; (ii) preventing access by those who are not entitled to access Information Assets and Information Systems; and (iii) protecting the environment through proper management and maintenance to allow for the reliable operation of the Information Assets and Information Systems.

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 ensure that their Information Systems are housed in a Designated Secure Computing Facility (DSCF) that meets the requirements of this policy.

2. Each Department and Unit Leader who oversees a DSCF, or rooms containing network equipment, wiring, or telecommunications, will:
    a. Develop technical procedures meet the Risk Controls set forth below when managing the security and environmental controls (e.g. HVAC, emergency power shut off, fire suppressant, humidity control, cabling, etc.).
    b. Develop procedures to all for the authorization of, and keep a record of the authorization, Covered Individuals who have a need to access the DSCF.
    c. Develop procedures for the revocation of access pursuant to other established policies.
    d. Ensure the housed Information Systems or Information Assets are physically secured in a manner that provides access to only those Covered Individuals they authorize.
    e. Ensure that all Covered Individuals within the DSCF are wearing the appropriate badge that distinguishes them between an employee and a visitor. All visitors will be identified as such with the appropriate badge. Temporary badges that provide access to the DSCF must expire after a set period of time.
    f. Review the physical security and environmental controls of the DSCF on a periodic basis, and consult with the CISO of their Organization, to ensure adherence to this policy.

g. Document repairs and modifications to the physical components of the facility which are related to security (e.g. hardware, doors, walls and locks).

3. Each IT Custodian is responsible for ensuring that Information Assets in public areas have the appropriate physical safeguards in place to prevent the theft of the Information Asset.

4. Each IT Custodian is responsible for ensuring that Information Assets in public areas used to process, store or transmit Protected Information is set up in a manner that prohibits the incidental viewing of the display screen.

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.

Physical and Environmental Protection Policy and Procedures (PE-1 C)

Core	The CISO of each Organization will define the proper physical and environmental controls, pursuant to this policy, which must be implemented by Information System Owners and IT Custodians.
Low	N/A
Moderate	N/A

Physical Access Authorizations (PE-2 CM)

Core	• Each DSCF, network, wiring or telecommunications room, must have access limited to only authorized individuals. • Access to the DSCF, network, wiring or telecommunications room, will be granted through a physical security system that provides access via badges. • When badge systems are not available for wiring or telecommunications room, access must be managed via key access. Key distribution and management must be maintained with proper documentation. • Access to the DSCF, network, wiring or telecommunications room, will be revoked immediately once it is no longer needed. • Authorized access to the DSCF, network, wiring or telecommunications room, will be reviewed annually.

Low	N/A
Moderate	Access to any DSCF will require two forms of identification which positively identifies the Covered Individual prior to access being granted to the individual's access badge.

Physical Access Control (PE-3 C)

Core	• Access to a DSCF must be protected through the use of a card reader. • Access to a network, wiring or telecommunications room should be protected through the use of a card reader, but may be limited to key or combination access if permitted by the Organizations' respective CISO. • Physical access audit logs to a DSCF, network, wiring or telecommunications room, will be maintained and recorded for all Covered Individuals, including visitors, and retained for at least 90 days. • Visitors to a DSCF, network, wiring, or telecommunications room, are escorted and visitor activity is monitored in all circumstances. • Secures keys, combinations, and other physical access devices to a DSCF, network, wiring or telecommunications room, must be inventoried. • Secures keys, combinations, and other physical access devices to a DSCF, network, wiring or telecommunications room, are changed when keys are lost, combinations are compromised or Covered Individuals with access to a combination is terminated or job duties change.
Low	N/A
Moderate	N/A

Access Control for Transmission Medium (PE-4 M)

Core	N/A
Low	N/A
Moderate	Locked wiring closets and disconnected spare jacks safeguards must be in place to control physical access to system distribution and transmission lines.

Access Control for Output Devices (PE-5 M)

Core	N/A
Low	N/A
Moderate	Information Assets with output devices (displays, monitors, printers, copiers, scanners, etc.) must be deployed in a manner that prevents unauthorized individuals from obtaining the output.

Monitoring Physical Access (PE-6 CL)

Core	Access to a DSCF: • Must be monitored to detect physical security incidents through the use of intrusion alarms (e.g. door open alarms, tampering alarms, etc.) and video surveillance equipment. • Physical access logs are reviewed periodically and for occurrence of any intrusion alarms. • Security incidents to the DSCF, wiring and telecommunication rooms must be reported to campus safety and the applicable Information Security Office.
Low	Video surveillance recordings must be kept for a period of ninety (90) days.
Moderate	N/A

Visitor Access Records (PE-8 LM)

Core	Visitor Access Records: • Must be maintained for a period of one (1) year • Must be reviewed on a periodic basis
Low	N/A
Moderate	N/A

Power Equipment and Power Cabling (PE-9 M)

Core	N/A
Low	N/A
Moderate	Power equipment and power cabling within a DSCF, network, wiring or telecommunications room, must be protected from damage and destruction.

Emergency Shutoff (PE-10 M)

Core	N/A
Low	N/A
Moderate	The DSCF: • Must contain a mechanism for shutting off power to Information Systems in emergency situations. • Must have emergency shutoff switches or devices in locations that facilitate

	safe and easy access for personnel. Emergency power shutoff must be protected from unauthorized and accidental activation.

Emergency Power (PE-11 M)

Core	N/A
Low	N/A
Moderate	The DSCF must contain short-term uninterruptible power supply to facilitate either an orderly shutdown of the information system OR transition of the information system to long-term alternate power in the event of a primary power source loss.

Emergency Lighting (PE-12 L)

Core	N/A
Low	The DSCF employs and maintain automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes.
Moderate	N/A

Fire Protection (PE-13 CM)

Core	The DSCF must contain, employ and maintain fire suppression and detection devices/systems that are supported by an independent energy source.
Low	N/A
Moderate	The DSCF employs an automatic fire suppression capability when it is not staffed on a continuous basis.

Temperature and Humidity Controls (PE-14 C)

Core	The DSCF must contain an environmental management system that continuously monitors and maintains temperature and humidity levels within the facility where Information Systems resides at a level consistent with ASHRAE Thermal Guidelines for Data Processing Environments.
Low	N/A
Moderate	N/A

Water Damage Protection (PE-15 C)

Core	The DSCF will employ safeguards that protect from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working

	properly, and known to key personnel.
Low	N/A
Moderate	N/A

Delivery and Removal (PE-16 LM)

Core	All movement of Information Systems and Information System components into and out of the DSCF, network, wiring or telecommunications rooms are authorized, monitored, and controlled.
Low	A record of the movement of Information Systems and Information System components into and out of the DSCF, network, wiring or telecommunications rooms are maintained.
Moderate	N/A

Alternate Work Site (PE-17 M)

Core	N/A
Low	N/A
Moderate	Procedures must be developed, documented, and implemented effectively to control security at alternate work sites which aligns with the Organizations' business continuity and contingency plans.

VI. Cross References

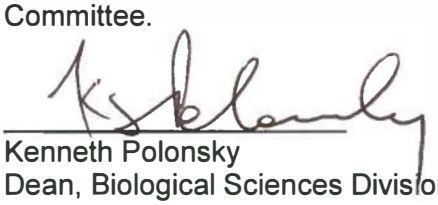
POL-AC Access Control Policy

VII. Policy References

HIPAA Security Rules: 42 C.F.R. § 164.310(a)

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	12/17/15