Cybersecurity Incident Response Policy

Policy 17	POL-IR	Effective Date	8/8/17	Review Date	8/8/17	Version	1.0

Table of Contents

I. Purpose 1
II. Scope 1
III. Policy 1
IV. Procedures 2
V. Risk Based Controls 9
Incident Response Policy and Procedures (IR-1 C) 9
Incident Response Training (IR-2 C) 9
Incident Response Testing (IR-3 M) 9
Incident Handling (IR-4 CM) 9
Incident Monitoring (IR-5 C) 10
VI. Cross References 11
VII. Policy References 11
VIII. Interpretation, Implementation and Revision 12
IX. Approval and Ownership 13
X. Revision History 13

I. PURPOSE

The purpose of this Policy is to describe the procedures to be followed to address a Cybersecurity Incident involving (a) Information Assets operated by the Organizations' Covered Individuals, or (b) the Organizations' Information that are transmitted, stored or processed on any Information Asset that is or may have been inappropriately accessed.

II. SCOPE

This policy applies to the Cybersecurity Incident Response functions of the BSD and UCMC (the Organizations). All Covered Individuals are subject to this policy.

III. POLICY

Every User of the Organizations' Information Assets and Information has responsibility to protect the privacy, security and integrity of the Information Assets and Information and to report concerns and cooperate with responders during and after Cybersecurity Incident investigations.

The Organizations will react effectively and quickly when investigating a Cybersecurity Incident by having established processes and channels of communication, defined response activities, defined roles and responsibilities, and assurances that regulatory and legal reporting requirements are met.

The general actions taken during a Cybersecurity Incident response are:

a. Detect and identify a suspected or known Cybersecurity Incident

b. Analyze and respond to suspected or known Cybersecurity Incidents

c. Contain actual or potential loss, corruption, inappropriate disclosure, inappropriate exposure, or breach of Information

d. Mitigate, to the extent practicable, harmful effects of Cybersecurity Incidents that are known to the Organizations or third parties with access to Information Assets and/or Information

e. Recover Information Assets and/or Information affected by the Cybersecurity Incident

f. Document Cybersecurity Incidents and their outcomes, including recommendations where appropriate

g. Support the Organizations' ability to fulfills its obligations under policy, contract, and federal and state laws with respect to actual and potential Cybersecurity Incidents

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

A. General Procedures

2. When an individual becomes aware of any actual or possible Cybersecurity Incident involving any UCMC or BSD Information Assets or information in electronic form, the individual is required to immediately (but no more than 24 hours) report to the following:

    a. for electronic information about patients, UCMC business or employees, clinical trials, or the clinical enterprise of the BSD, the UCMC ISO.

    b. for electronic BSD employee, student, or BSD business (e.g. finance, Human Resources) information, or basic science research information, the BSD ISO.

    If information does not fall into one of the two preceding categories, or the individual does not know whether the information falls into one of the two preceding categories, then:

    c. for UCMC operated Information Systems, the UCMC ISO

    d. for BSD operated Information Systems, the BSD ISO

    If it is unclear as to whether a situation should be considered a Cybersecurity Incident, the UCM Chief Information Security Officer should be contacted to evaluate the situation.

3. The UCMC and BSD Security Offices, as appropriate, are primarily responsible for the coordination and investigation of all Cybersecurity Incident response activities within the Organizations. The nature of the Information Systems and information involved or potentially affected by the Cybersecurity Incident will dictate whether the UCMC CISO or BSD CISO will serve as the lead (referred to as the "**Lead CISO**"). In general, the CISOs will follow the notification guidance outlined in section A.1 above to predetermine the responsible CISO who will act as the Lead CISO. The respective CISOs will agree which office will take the lead on any particular response.

4. Business Associate Agreements will contain a term that requires the business associate to notify the Privacy Officer of a Cybersecurity Incident and cooperate with the

Organizations in the investigation and response to the Cybersecurity Incident. The Privacy Officer will consult with the applicable CISO and either the UCM Office of Legal Affairs or the University Office of Legal Counsel as necessary to evaluate the report and determine its role in the business associate's investigation, analysis and response. Any individual who receives a notification of a Cybersecurity Incident by a third party must immediately forward the notification to the Privacy Officer.

5. The CISOs of the Organizations may also identify an actual or potential Cybersecurity Incident through their proactive monitoring of the Organizations' network and Information System activities.
6. Once identified, the Lead CISO will use standard internal procedures to log and track Cybersecurity Incidents and, working with others as appropriate, take steps to investigate, escalate, remediate, refer to others or otherwise address as outlined in this Policy.
7. Each Department or Unit Leader is expected to comply with instructions from the Lead CISO during a Cybersecurity Incident.

B. Cybersecurity Emergency Response Team:

1. The purpose of the Cybersecurity Emergency Response Team (CERT) is to supplement the information security infrastructure and minimize the threat of damage resulting from Cybersecurity Incidents.
2. The Chief Privacy Officer, either CISO, or the Office of Legal Counsel (and their delegates) can call a CERT as defined in D.1. The team's work is Restricted Information, meaning it may not be shared outside of the team. CERT members will share information about Cybersecurity Incidents outside of the team only (a) on a need-to-know basis, and (b) after consultation with and approval of the Lead CISO.
3. The CERT, led by the Lead CISO, is responsible for leading the investigation of the Cybersecurity Incident, assessing the Cybersecurity Incident, and advising on the remediation plan.

C. Responsibilities:

1. All individuals responding to a Cybersecurity Incident will work collaboratively with the goal of completing the assessment and remediation as quickly as possible.
2. The CISOs for the Organizations are responsible for leading Cybersecurity Incident assessments and responses that involve the potential compromise of an Information Assets and electronic Information. The CISOs will not be responsible for leading privacy incidents or breaches that leverage electronic Information or Information Assets. Some examples of these cases, which will be led by the Privacy Program, are:
    a. an errant email, fax, text, phone call or other message
    b. viewing of patient information without a need to know (referred to as "snooping")
3. The Lead CISO will oversee and guide the incident management process to promote a coordinated, consistent, efficient, and effective response. He or she will communicate the Cybersecurity Incident to appropriate personnel and maintain contact, for the purpose of update and instruction, for the duration of the Cybersecurity Incident.

4. Although the Lead CISO will coordinate Cybersecurity Incident response, responsibility for the Cybersecurity Incident remains with the unit experiencing the Incident, and it must allocate unit resources to resolve the Cybersecurity Incident in a cooperative and timely manner.
5. The Lead CISO, in concert with the Privacy Program and the UCM Office of Legal Affairs, will complete the risk assessment and ensure compliance with applicable breach notification laws and regulations, including any required notifications of individuals and/or regulatory or government officials.
6. The UCM Office of Legal Affairs is responsible for providing legal counsel and advice, in cooperation and consultation with the University of Chicago Office of Legal Counsel as appropriate. Outside legal advice may only be obtained through the Office of Legal Affairs.
7. The CERT is comprised of two layers:
    a. Primary team, which is comprised of the Lead CISO, the Privacy Program if the Cybersecurity Incident involves PHI or PII, and the UCMC Office of Legal Affairs, in cooperation with the University of Chicago Office of the General Counsel as appropriate.
    b. Secondary team, which is called on an ad hoc basis to incorporate subject matter experts as needed. The experts include but are not limited to leaders from:
        i. UC and UCM Marketing and Communications
        ii. University of Chicago Insurance and Risk Management
        iii. UCMC Human Resources or BSD Human Resources
        iv. CBIS, Departmental IT, or ITS
        v. Leadership of the affected Department or Unit
        vi. Other subject matter experts identified by the primary incident response team

    The UCMC Office of Legal Affairs will determine if a secondary team is needed, and will determine, with the input of the Lead CISO, which experts to include. The team will leverage and coordinate the experience, expertise, and resources of other departments as necessary and appropriate.
8. The University of Chicago Director of Risk Management will serve as the primary contact with the Organizations' insurer.
9. Marketing and Communications will review and approve any external communication regarding the Cybersecurity Incident. It will keep the University of Chicago Communications Office apprised.
10. Each of the Lead CISOs and the Privacy Officer will ensure appropriate information and evidence related to their respective scopes of the investigation and remediation is collected on the Organizations' standardized documentation and logged.
11. The Lead CISO is responsible for instructing the Information System Owner of the necessary remediation of computer and electronic communication-based resources affected by the Cybersecurity Incident. The Lead CISO will prescribe the replacement devices and security services necessary to remediate the problem.

D. Cybersecurity Incident Response:

1. When a Cybersecurity Incident is reported, the recipient of the report will immediately invoke the incident response procedures commensurate with the gravity of the situation.
    a. A Minimal, Low or Medium Severity situation will be handled by the Lead CISO or Privacy Program, as appropriate, without the need to invoke the CERT. The Office of Legal Affairs will be consulted as needed.
    b. For all other severities, in accordance section B above, the Lead CISO receiving the report will invoke the primary CERT, which will have an initial immediate conversation to review the facts and agree upon a response plan for the particular incident.
2. The Lead CISO, or their delegate, is responsible for:
    a. logging the Cybersecurity Incident
    b. leading and documenting the investigation of the Cybersecurity Incident
    c. leading the process to gather facts relating to the Cybersecurity Incident
    d. leading the process to assess the facts gathered of the Cybersecurity Incident
    e. taking direction from the UCM Office of Legal Affairs to support the provision of legal advice
    f. keeping the secondary incident response team, if any, and other leadership informed of the status of the assessment, investigation, and remediation
    g. scheduling the meetings of the CERT, which shall be as frequent as necessary (but typically daily)
    h. If necessary and upon legal advice, communicating with an outside forensic expert
3. The CERT will develop an appropriate incident response plan based upon the initial report, adjust and update the plan as more information is gathered, and carry out the plan and its responsibilities listed above in an expeditious manner.
4. In order to minimize the impact of the Cybersecurity Incident or to complete a proper investigation, the Lead CISO, upon the advice of the Office of Legal Affairs, has the authority to restrict information system access or operations to protect against unauthorized Information disclosures. As required, the Lead CISO may take extraordinary measures to protect the enterprise during an active Cybersecurity Incident. Examples include, but are not limited to: blocking threat actors, removing systems from the network, blocking protocols, applications, or services, requiring stricter security controls enterprise wide, or installing software enterprise wide.
5. The Lead CISO will immediately advise and assist in:
    a. Eradicating the Cybersecurity Incident and its impact, including containing and limiting any loss, corruption, inappropriate disclosure, inappropriate exposure, or breach resulting from the Cybersecurity Incident.
    b. Restoring or replacing systems and devices affected by the Cybersecurity Incident when it is safe and appropriate to do so. The impact of the loss of a system or device will determine the priority of the action to be taken.
6. Based upon the respective CISOs' incident response plan, the facts surrounding the Cybersecurity Incident will be investigated to identify the cause of the Cybersecurity

Incident, the technical impact of the incident, the scope of the technical impact, the remediation necessary to contain the impact, the impact on the originators of any Information (both individuals and entities), and, when appropriate, the need for breach notification.

7. The CERT will evaluate and analyze the technical implications of the Cybersecurity Incident, assess the risk to systems, information, people, and entities, assess the impact of the Cybersecurity Incident, and reach conclusions about the Cybersecurity Incident, including, for example, whether the Cybersecurity Incident has resulted in a breach (as defined by state or federal law). For Cybersecurity Incidents that involve PHI, this breach evaluation must take place within 7 days of notification of the Incident.
8. If the Cybersecurity Incident results in a significant impact, or creates a serious threat to the institution or the subjects of the Information, or result in potential other risks, the Lead CISO will notify the CERT promptly. If a governmental entity reported the Cybersecurity Incident, the Lead CISO will notify the UCMC Vice President and General Counsel and the UCMC Chief Compliance Officer immediately.
9. The Privacy Program, UCMC Information Security Office, and BSD Information Security Office will collaborate on reporting systemic problems, educating individuals who may have caused the Cybersecurity Incident, and advising the respective human resources offices on corrective action.

E. Regulatory Reporting and Notification:

1. The UCM Office of Legal Affairs will advise the CERT of the regulatory obligations to report the results of a Cybersecurity Incident and/or notify those who may be at risk. The factors that will be used include:
    - legal duty to notify
    - length of compromise
    - character and nature of the human involvement in the Cybersecurity Incident
    - sensitivity of data
    - existence of evidence that data was accessed and acquired
    - existence of evidence that supports the intent of actions that led to the system or device compromise
    - additional factors recommended for consideration by members of the Incident Response Team or senior leadership
2. The UCM Office of Legal Affairs will provide to the Privacy Program, Information Security Officers, and senior leadership legal advice concerning breach notification, including the requirements under federal and state law. The advice will come in the form of general guidance as well as incident-specific legal analysis, which will be based upon the facts gathered and, as applicable, the input of the CERT. The Privacy Program will carry out the breach notification process for breaches of PHI and PII. The UCMC Office of Legal Affairs and the Chief Compliance Officer will determine who is responsible for Cybersecurity Incident notification not involving PHI and PII.

F. Law Enforcement Notification:

The UCMC Office of Legal Affairs will determine a) if law enforcement is to be notified of a Cybersecurity Incident and b) the responsible party for making the notification. The following individuals may be consulted and included in the decision to notify law enforcement:

- President, University of Chicago Medical Center
- Richard T. Crane Distinguished Service Professor, Dean and EVP for Medical Affairs
- UCM's VP and Chief Information Officer, in consultation with the BSD Chief Research Informatics Officer as appropriate
- UCM VP and Chief Compliance Officer
- UCM's VP and General Counsel, in consultation with the University of Chicago General Counsel as appropriate

Other key stakeholders should be consulted as appropriate.

G. Debrief and Identify System Problems:

As necessary, the Lead CISO will schedule a debriefing meeting with the unit and the Incident Response Team after completion of the response to ensure appropriate corrective action in the unit or department is taken, to identify any actions that could be taken to reduce the likelihood of a future similar incident, and to continuously improve the response processes. The Lead CISOs will make long-term remediation recommendations to the Privacy and Security Steering Committee and/or the Executive Cyber Risk Committee.

H. Documentation:

1. Each CISO and the Privacy Officer will ensure that Cybersecurity Incidents and their resolutions are appropriately logged as an incident ticket. The ticket entries will include the date the Cybersecurity Incident was reported, the name and title of the reporter, and the department and/or unit affected. The log will be updated through the completion of the response process with the following: investigation notes, containment actions, and response actions.
2. The Lead CISO shall issue an Incident Report for every Cybersecurity Incident for which the CERT is called, as well as Cybersecurity Incidents in which the Lead CISO, in his or her judgement, determines that a Cybersecurity Incident response is necessary. The Incident Report will include: incident number, incident severity, contact and resolution dates, timelines, data involved (including whether PHI or PII is involved), number of individuals affected, the Information System Owner, Cybersecurity Incident narrative, the details of the Cybersecurity Incident and its cause, remediation and recommendations. The report will be distributed to the Incident Response Team and potentially the responsible Executive Managers.
3. The Lead CISO, or their delegate, will document the deliberations and decision of the CERT as well as all actions taken pursuant to the deliberations. Cybersecurity Incident statistics and reporting will be provided to the Privacy and Security Steering Committee

I. Preserving Evidence:

The Lead CISO will consult with the UCM Office of Legal Affairs to seek advice regarding the preservation of evidence of Cybersecurity Incidents. Upon advice of legal counsel, or in accordance with Incident Response plans, equipment and devices will be sequestered and preserved (a) if necessary to properly investigate the Cybersecurity Incident and/or (c) professional determination and forensic best practices. Sequestered equipment and devices will be held under lock and key until a release is authorized by the Lead CISO, upon advice of legal counsel. A chain of custody will be kept for Cybersecurity Incident involving the preservation of evidence. If necessary, the Lead CISO will direct his or her team to copy computer data in a forensically sound practice to preserve evidence; copying may include using utilities that will produce an exact forensically sound image with verifiable authenticity.

J. Miscellaneous:

1. The department or unit that is the source of the Cybersecurity Incident will be responsible for the costs associated with third party experts, outside legal counsel and breach notification.
2. Pursuant to the POL-RO Roles and Responsibility Policy, the Lead CISOs may disconnect Information Resources that present a security risk from the UCMC or University network.

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

V. RISK BASED CONTROLS

Incident Response Policy and Procedures (IR-1 C)

Core	The CISO of each Organization will define the proper incident response controls, pursuant to this policy.
Low	N/A
Moderate	N/A

Incident Response Training (IR-2 C)

Core	The CISOs of each Organization will ensure that incident response training has been given to System Owners who: • Have assumed an incident response role or responsibility for that Information System • When required by changes to Information System management
Low	N/A
Moderate	N/A

Incident Response Testing (IR-3 M)

Core	N/A
Low	N/A
Moderate	The Cybersecurity Incident Response processes and procedures will be tested on an annual basis for those Information Systems to ensure the protection of systems that contain RESTRICTED Information, or support mission critical functions of the Organizations. Cybersecurity Incident Response plans are tested with other Business Continuity and Emergency Operations plans.

Incident Handling (IR-4 CM)

Core	The CISOs will: • Implement incident handling capabilities for Cybersecurity Incidents that includes preparation, detection and analysis, containment, eradication and recovery • Coordinate cyber incident handling activities with contingency planning activities; and • Incorporate lessons learned from ongoing cyber incident handling activities into incident response procedures, training, and testing and implement the resulting changes accordingly.
Low	*N/A*

Moderate	Cybersecurity Incident Response processes are managed through automated online incident management systems.

Incident Monitoring (IR-5 C)

Core	The CISOs will track and document Cybersecurity Incidents.
Low	*N/A*
Moderate	*N/A*

VI. Cross References

Policy A05-20, Mitigation and Breach Notification Policy
POL-RO Roles and Responsibilities Policy

VII. Policy References

45 CFR Section 164.304.
45 CFR Section 164.308(a)(6).
45 CFR Section 164.314(a)(2)(i)(C) & (b)(2)(iv).
HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414
Illinois Personal Information Protection Act, 815 ILCS Section 530/1 *et seq.*

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	6/29/17
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