Table of Contents

I. Purpose .......................................................................................................................... 1
II. Scope .............................................................................................................................. 1
III. Policy ............................................................................................................................ 1
IV. Procedures ..................................................................................................................... 2
   A. Training and Awareness Leadership ........................................................................... 2
   B. Current Employees, Members of Workforce, and Third Parties ............................... 2
   C. New Employees, New Members of Workforce, and New Third Parties ................. 2
   D. Documentation ......................................................................................................... 2
V. Risk Based Controls ...................................................................................................... 3
   Security Awareness and Training Policy and Procedures (AT-1 C) .............................. 3
   Security Awareness Training (AT-2 LM) ...................................................................... 3
   Role Based Security Training (AT-3 LM) ...................................................................... 3
   Security Training Records (AT-4 LM) ........................................................................ 4
VI. Policy References ......................................................................................................... 4
VII. References ................................................................................................................... 4
VIII. Interpretation, Implementation and Revision ............................................................. 5
IX. Approval and Ownership ............................................................................................. 6
X. Revision History ............................................................................................................. 6

I. Purpose

The UChicago Medicine (including UCMC, The Care Network and the UCM Community Health and Hospital Division) and the Biological Sciences Division of The University of Chicago (the “Organizations”) protects information and Information Assets that are the subject of legal, contractual, or enterprise confidentiality and security requirements (collectively the “Security Obligations”). The Organizations train Covered Individuals, on the policies and procedures, to promote a secure environment and the Acceptable Use of technology, as necessary and appropriate for the individuals to carry out their specific functions in accordance with the Security Obligations.

II. Scope

All Covered entities under the Organizations who use, store, process and transmit Organization’s information, are subject to this policy.

III. Policy

The Privacy Officer over each area, in consultation with the legal department, will determine whether non-employed individuals are members of the Organization’s Covered Individuals.

Each Organization’s Chief Information Security Officer, in consultation with the UChicago Medicine Office of Corporate Compliance and the legal department, determines the content, scope, and delivery mechanism(s) of awareness campaigns and training regarding information security consistent with each Organization’s Security Obligations (“Security Training”). Covered Individuals are required to participate in Security Training that is relevant and necessary to carry out their duties and responsibilities.
Capitalized terms used in this policy are defined in the glossary attached. The UChicago Medicine and BSD CISOs may change the definitions as necessary without the approval of the Cyber Security Executive Committee.

IV. PROCEDURES

A. Training and Awareness Leadership

The Organizations delegate to the CISOs the responsibility for Security Training content and working with departments to ensure Security Training content is included in the Organizations’ Security Training activities and programs. The CISOs will ensure that the Security Training content complies with other policies of the Organizations. Additionally, the CISOs shall align the Organization’s Security Training content.

B. Current Employees, Members of Workforce, and Third Parties

Each CISO will provide and/or facilitate, and each Covered Individual will participate in, Security Training related to the Organization’s information and use of Information Assets on at least an annual basis. Additional Security Training to Covered Individuals will be provided at the discretion of the CISOs, Privacy Officer, or legal counsel:

a) In response to an incident,

b) Based upon the individual’s role or function,

c) Based upon the content of the Restricted and Internal Information,

d) As needed to ensure the Organizations adhere to the Security Obligations. A CISO may delegate the Security Training of third parties to their employer, and require affirmation of completion of the Security Training. Each Covered Individual notified by the Organizations will actively participate in the Security Training as directed by their supervisor or other leader.

C. New Employees, New Members of Workforce, and New Third Parties

Each CISO will provide Security Training, to all new Covered Individuals, within their purview. Each Covered Individual will participate in their respective training. A CISO may delegate the Security Training of third parties to their employer, and require affirmation of completion of the Security Training. There is a variety of training methods available including instructor-led sessions, computer-based modules and guidance documents.

D. Documentation

Each CISO will document, or ensure that the department offering the Security Training documents the time, date, place, the individuals and the content of each Security Training session. The CISOs will maintain, or direct the department offering the Security Training to maintain documentation in the Security Compliance Program education files for six (6) years and make it available for inspection by regulatory authorities and each Organization’s leadership as appropriate.

The Organizations will use the Risk Based Controls below to implement the procedures.
V. **RISK BASED CONTROLS**

Core controls, designated as “C”, are mandatory and required across the operating environment. Low controls, designated as “L”, and Moderate controls, designated as “M”, shall be evaluated through as defined by the impact analysis and subsequent risk analysis.

**Security Awareness and Training Policy and Procedures (AT-1 C)**

| Core | • The Organizations delegate to the CISOs the responsibility for developing Security Training content and working with departments to ensure appropriate training content is included in the Organizations’ training activities and programs. The CISOs will ensure that the Security Training content complies with the other policies of the Organizations. In addition, the CISOs will ensure that each Organization’s Security Training content and programs are consistent and not conflicting.  
  • Supporting procedures shall facilitate the implementation of this policy. These procedures are subject to review and update no less than once per year. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>N/A</td>
</tr>
<tr>
<td>Moderate</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Security Awareness Training (AT-2 LM)**

| Core | • Security Training is included for new users to the Organization as part of the New Employee Orientation program.  
  • Training will include the methods for Users to report Security Incidents |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>• Where possible and practical, Security Training includes practical exercises that simulate actual cyber-attacks, such as simulating phishing attacks for Covered Individuals.</td>
</tr>
</tbody>
</table>
| Moderate | • Security Training includes content towards recognizing and reporting potential indicators of insider threat.  
  • Access to Information Systems is restricted until Covered Individuals have completed Security Training. |

**Role Based Security Training (AT-3 LM)**

<table>
<thead>
<tr>
<th>Core</th>
<th>• Certain Covered Individuals, such as those who process credit cards, receive Security Training specific to their business function on an annual basis.</th>
</tr>
</thead>
</table>
| Low | • IT Custodian's receive appropriate Security Training as it relates to the security management and operations of their Information Systems.  
  • The IT Custodian acknowledges having received the Security Training either in writing or electronically as part of the training course completion. |
Security Training Records (AT-4 LM)

| Core | • Security Training records for New Employee Orientation, full Covered Individual annual Security Training and Role Based Security Training are documented and monitored.  
|      | • Training records are retained for a period of 6 years from the date of its creation. |
| Low  | N/A |
| Moderate | N/A |

VI. POLICY REFERENCES

POL-RO Security Responsibilities and Oversight Policy
POL-AC Access Control Policy

VII. REFERENCES

HIPAA Security Rules: 42 C.F.R. § 164.308(a) (5)
NIST: Awareness and Training (AT)
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 and EVP Medical Affairs, Biological Sciences Division

Sharon O'Keefe
President, The University of Chicago Medical Center
Security Awareness and Training Policy

<table>
<thead>
<tr>
<th>Policy</th>
<th>POL-IA</th>
<th>Effective Date</th>
<th>Review Date</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td></td>
<td>9/22/2015</td>
<td>9/6/2018</td>
<td>2.0</td>
</tr>
</tbody>
</table>

# IX. APPROVAL AND OWNERSHIP

<table>
<thead>
<tr>
<th>Owner</th>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy &amp; Security Steering Committee</td>
<td>Policy Development Group</td>
<td>6/12/15</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Approved By</th>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kenneth Polonsky, MD</td>
<td>Richard T. Crane Distinguished Service Professor, Dean and EVP for Medical Affairs</td>
<td>9/22/15</td>
</tr>
<tr>
<td>Sharon O’Keefe,</td>
<td>President, University of Chicago Medical Center</td>
<td>9/22/15</td>
</tr>
</tbody>
</table>

# X. REVISION HISTORY

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
<th>Review Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Initial Version</td>
<td>9/22/15</td>
</tr>
<tr>
<td>2.0</td>
<td>Inclusion of Ingalls, editorial edits</td>
<td>9/6/2018</td>
</tr>
</tbody>
</table>