I. Purpose ......................................................................................................................................... 1
II. Scope .......................................................................................................................................... 1
III. Policy .......................................................................................................................................... 2
IV. Procedures ................................................................................................................................... 2
V. Risk Based Controls...................................................................................................................... 3
   Identification and Authentication Procedures (IA-1 C)................................................................. 3
   Identification and Authentication of Organizational Users (IA-2 CLM)........................................ 3
   Device Identification and Authentication (IA-3 M)............................................................... 4
   Identifier Management (IA-4 C)................................................................................................. 4
   Authentication Management (IA-5 CLM)..................................................................................... 4
   Authenticator Feedback (IA-6 C)............................................................................................... 5
   Cryptographic Module Authentication (IA-7 C)........................................................................... 6
   Identification and Authentication of Non-Organizational Users (IA-8 CL)............................... 6
   Service Identification and Authentication (IA-9 CL)..................................................................... 6
VI. Definitions .................................................................................................................................... 7
VII. Cross References ......................................................................................................................... 7
VIII. Policy References ....................................................................................................................... 7
IX. Interpretation, Implementation and Revision .............................................................................. 8
X. Approval and Ownership ............................................................................................................... 9
XI. Revision History .......................................................................................................................... 9

I. PURPOSE

The University of Chicago Medicine (including UCMC, UCM 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 is the subject of legal, contractual, or enterprise confidentiality and security requirements (collectively the “Security Obligations”) Access to information and Information Systems will be limited to only properly identified and authorized users, processes acting on behalf of users (such as service accounts), or devices and only after ensuring proper identification and authentication of its users, service accounts, processes or devices.

This policy sets forth a general framework for identification, user account creation, authentication requirements and service account management and sets the rules under which systems shall operate to reduce the risk, and minimize the effect of security incidents.

II. SCOPE

This policy applies to Information Systems used to store, process and transmit the Organization’s Information. All Covered Individuals are subject to this policy.
III. **Policy**

Covered Individuals who access Information Systems and information may do so with the proper identification, authentication and authorization. Access rights are determined based upon the Security Obligations.

Access is subject to privacy laws and policies as well as contractual obligations.

IV. **Procedures**

1. The UChicago IAM Program establishes the policies and systems for the management of unique identifier, called the ChicagoID, to each Covered Individual and User within the Organizations. The UChicago IAM program and the UCM IAM program will each create the unique identifier for new Covered Individuals congruent to the policies set by UChicago. The ChicagoID is a serialized alphanumeric that is unique to each individual, similar to a social security number.

2. IT Custodians will establish one or more user accounts for each Covered Individual that will be used throughout the Organizations. The user name of the account will be consistent and unique across the Organizations and follow these rules:
   
   a. If a User joins UChicago and establishes a user account through its processes (such as the CNETID) then this account name will be used for any and all accounts created across the UChicago and UCM.
   
   b. If a User joins UCM and establishes an account through its processes (such as the UCHADID), then this identifier will be used for any and all accounts created across the UChicago and UCM.

   At no time will the user names be deleted, changed or destroyed.

3. System Owners and IT Custodians will ensure user accounts are linked to the ChicagoID.

4. System Owners and IT Custodians are responsible for managing Non-Human Credential or Service Accounts, such as privileged accounts that are for administrative purposes, may be used only when the following controls are set:

   a. All Service Accounts must follow a standard naming convention set forth by the CISOs of the Organizations

   b. A record of approved Service Accounts must be maintained by the appropriate System Owners and IT Custodians, and kept at a minimum for a period of six (6) years beyond the use of the account. This log must contain the following elements:
      
      i. Name of the account
      ii. Username of the account (if different from name)
      iii. Date/Time of the request
      iv. Date/Time of account creation
v. Individual requesting the account
vi. The account owners of the Service Account, with their corresponding ChicagoID logged and linked to the Service Account.

vii. Department of the requester
viii. Contact information for the department (or user's manager)
ix. Purpose of the account, not limited to the System its supporting and the functions in that system required by the account

c. Will configure the Service Accounts to log in accordance to security policies and standards.

Except in the cases of normal operational practices, such as the use of quality assurance and testing, disable the use of Interactive terminal sessions with Service Accounts

d. Service Account passwords must be a minimum of 60 randomly generated complex characters, or the maximum length supported by the application/system, whichever is shorter

e. May only leverage appropriate CISO’s authorized credential service and authentication source

5. The CISOs will ensure authentication and authorization mechanisms are congruent to the established direction provided by the defined IT governance processes.

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.

Identification and Authentication Procedures (IA-1 C)

<table>
<thead>
<tr>
<th>Core</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The CISO of each Organization define identification and authentication that each Information System Owner will implement. The Information System Owner will identify the individuals, groups of individuals or roles of individuals, who may access the Information System with Information under his/her control, and for each, the appropriate access level. The identification of the individuals, groups and roles with their permitted access levels will be documented by the Information System Owner; all access management activity will be documented.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Low</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Moderate</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Identification and Authentication of Organizational Users (IA-2 CLM)
Identification and Authorization Policy

<table>
<thead>
<tr>
<th>Core</th>
<th>Each Covered Individual must be uniquely identified and authenticated when accessing any Organizational Information System.</th>
</tr>
</thead>
</table>
| Low  | - Multifactor authentication is used for privileged accounts  
       - Multifactor authentication is used for remote, off-campus, access to non-privileged accounts  
       - Those authorized to use privileged accounts must leverage separate and distinct accounts for their privileged purposes. These accounts must be separate from regular user accounts (non-privileged accounts). |
| Moderate | N/A |

### Device Identification and Authentication (IA-3 M)

<table>
<thead>
<tr>
<th>Core</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>N/A</td>
</tr>
<tr>
<td>Moderate</td>
<td>Organizationally owned devices are uniquely identified and authenticated prior to the device being used to establish a remote network connection, where possible.</td>
</tr>
</tbody>
</table>

### Identifier Management (IA-4 C)

| Core | Information System identifiers are managed in the following manner:  
       - All Covered Individuals must have a ChicagoID unique identifier.  
       - User accounts must be unique  
       - User accounts must be linked to the ChicagoID  
       - Any non-privileged account (e.g. user account) where the password is shared with more than one individual must be cleared with the CISO of that respective Organization prior to its establishment  
       ChicagoID and user accounts are not permitted to be reassigned to another individual |
<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>

### Authentication Management (IA-5 CLM)

| Core | Authentication assurances are handled in the following manner:  
       - Passwords:  
         - Delivered to Users during the onboarding processes  
         - If forgotten, will be managed first via self-service password management capabilities, secondarily by the service desk |
|------|--------------------------------------------------------------------------------------------------|
### Identification and Authorization Policy

<table>
<thead>
<tr>
<th>Classification: Internal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Page 5 of 9</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>POL-IA</th>
<th>Effective Date</th>
<th>Review Date</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>9/6/2018</td>
<td>9/6/2018</td>
<td>1.0</td>
</tr>
</tbody>
</table>

- If compromised, the user account will be disabled or password changed promptly
  - Soft-tokens and hardware-based tokens for Two Factor Authentication
    - Delivered to Users during the self-service enrollment process via 2fa.uchicago.edu
    - If forgotten, will be managed by a call to the service desk
    - If compromised, the user account will be disabled or password changed promptly
    - Hard-tokens will be provisioned only upon personal photo verification leveraging either: driver’s license, state-sponsored ID, or UChicago badge.
  - At no time will a User be permitted to change their ChicagoID.

### Low

For password-based authentication:
- Meets all the password-based Access Control controls noted above
- Must be stored and transmitted by leveraging cryptography
- Allows for the use of a temporary password as long as it is forced to immediately change to a permanent password after logon.

For software and hardware-based tokens:
- All tokens will meet assurance as defined by a FIPS 140-2 approved algorithm
- Soft-tokens will be provisioned via the self-service portal: 2fa.uchicago.edu

### Moderate

For PKI-based authentication:
- Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information
- Enforces authorized access to the corresponding private key
- Maps the authenticated identity to the account of the individual or group
- Ensures the implementation of a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network

---

**Authenticator Feedback (IA-6 C)**

<table>
<thead>
<tr>
<th>Core</th>
<th>The Information System is configured to obscure password inputs such that it prevents shoulder surfing.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>N/A</td>
</tr>
<tr>
<td>Moderate</td>
<td>N/A</td>
</tr>
</tbody>
</table>
## Identification and Authorization Policy

### Cryptographic Module Authentication (IA-7 C)

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Core</strong></td>
<td>Encryption is configured for authentication processes both in transit and at rest. Refer to POL-SC (Risk Based Controls SC-12 and SC-13) for implementation specifications.</td>
</tr>
<tr>
<td><strong>Low</strong></td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Moderate</strong></td>
<td>N/A</td>
</tr>
</tbody>
</table>

### Identification and Authentication of Non-Organizational Users (IA-8 CL)

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Core</strong></td>
<td>All Non-Organizational Users will be uniquely identified.</td>
</tr>
<tr>
<td><strong>Low</strong></td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Moderate</strong></td>
<td>N/A</td>
</tr>
</tbody>
</table>

### Service Identification and Authentication (IA-9 CL)

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Core** | All Service Accounts must follow a standard naming convention set forth by the CISOs of the Organizations. A record of approved Service Accounts must be maintained by the appropriate System Owners and IT Custodians, and kept at a minimum for a period of six (6) years, or while in use, whichever is longer. This log must contain the following elements:  
- Name of the account  
- Username of the account (if different from name)  
- Date/Time of the request  
- Date/Time of account creation  
- Individual requesting the account  
- Department of the requester  
- Contact information for the department (or user's manager)  
- Purpose of the account, not limited to the System its supporting and the functions in that system required by the account  

Use of the Service Account must log:  
- The action performed  
- The user on behalf of the action being performed by the Service Account  
- The date/time the action was performed  
- Any other information related to the context of the request that might be relevant, such as remote IP address, username, etcetera  

Service Account passwords must be a minimum of 60 randomly generated complex characters, or the maximum length supported by the application/system, whichever is shorter |
| **Low** | N/A |
| **Moderate** | N/A |
VI. **DEFINITIONS**

**Non-Human Credential or Service Account:** Any single or combination of username/password, certificate, token, or other means utilized by a non-human actor to gain access to an electronic or networked resource.

VII. **POLICY REFERENCES**

- POL-RO Responsibility and Oversight Policy
- POL-AC Access Control Policy
- POL-SC Systems and Communication Protection Policy

VIII. **REFERENCES**

HIPAA Security Rules: 42 CFR §:
- 164.308(a)(4)
- 164.308(a)(5)(ii)(D)
- 164.312
- 164.312(d)
- 164.312(a)(2)(i)

NIST: Access Control (AC)
IX. 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
Identification and Authorization Policy

<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>7/6/2018</td>
</tr>
<tr>
<td>Kenneth Polonsky, MD</td>
<td>Richard T. Crane Distinguished Service Professor, Dean and EVP for Medical Affairs</td>
<td>9/6/2018</td>
</tr>
<tr>
<td>Sharon O'Keefe, RN</td>
<td>President, University of Chicago Medical Center</td>
<td>9/6/2018</td>
</tr>
</tbody>
</table>

XI. 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>9/6/2018</td>
</tr>
</tbody>
</table>