1.0 Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author(s)</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>06/22/2015</td>
<td>Katie Fleischman, Annie Garcia, Vincent Sposato</td>
<td>Initial draft of policy</td>
</tr>
<tr>
<td>2.0</td>
<td>10/17/2017</td>
<td>Lane Blanchard</td>
<td>Adopted CQM Initial draft as baseline</td>
</tr>
</tbody>
</table>

2.0 Policy Approval

Name of Approver: Ian Tebbett
Title of Approver: Assoc. Dean, Entrepreneurial Programs and IT
Approval Date: 04/24/2018

3.0 Purpose

The UF College of Pharmacy maintains large amounts of personal and restricted information. Information security is essential for protecting the interests and confidentiality of the UF COLLEGE OF PHARMACY, its personnel, clients, and customers. Information security cannot be achieved by technical means alone. Information security must also be applied and enforced by individuals, and this policy addresses security issues related to individuals including third party access to UF COLLEGE OF PHARMACY data and information systems (i.e. contractors, service providers, and partners).
This policy includes 3 key stages of a user’s access to information or information systems used in delivery of UF COLLEGE OF PHARMACY business services:

**Stage 1 - Provisioning of User Access** – Prior to provisioning access to information or information systems, background checks must be made to ensure that the individual is suitable for access to UF COLLEGE OF PHARMACY information systems.

**Stage 2 - Maintenance of User Access** – During the access period to information or information systems - users must be trained and equipped to use systems securely and their access must be regularly reviewed to ensure it remains in compliance.

**Stage 3 - Termination of User Access** - When a user’s requirement for access to information or information systems ends (i.e. when a user terminates their employment with the UF COLLEGE OF PHARMACY, or changes their role so that access is no longer required) - access needs to be removed in a controlled manner.

### 4.0 Policy Details

#### 4.1 Stage 1 Provisioning of User Access

4.1.1 Prior to Employment

The UF COLLEGE OF PHARMACY must ensure that potential employees are recruited in line with the UF COLLEGE OF PHARMACY’s core job requirements for the roles they are considered for and to reduce the risk of theft, fraud or misuse of information or information systems. These requirements are corporate in nature.

4.1.2 Roles & Responsibilities

Decisions on the appropriate level of access to information or information systems for a particular user are the responsibility of the UF College of Pharmacy Human Resources Department, as well as, the particular Data Owner(s).

Managers are responsible for ensuring that creation of new users, changes in role, and termination of users are submitted to the UF COLLEGE OF PHARMACY’s IT Helpdesk in a timely manner, using an agreed upon process.

The information security responsibilities of users must be defined and documented and incorporated into induction processes and contracts of employment. At a minimum, this will include:

- A statement that every user has been made aware and understands, the following UF COLLEGE OF PHARMACY policies
4.1.3 User Screening

Background verification checks must be carried out on all potential users, in accordance with all relevant laws, regulations, and ethics. The level of such checks must be appropriate to the business requirements, the classification of the information to be accessed, and the risks involved. These background checks should be in compliance with IT-SEC-0011 Background Investigation Policy.

Employment may begin prior to background verification being completed for orientation purposes only, but access to information systems or restricted information will not be granted until background clearance has been verified. Said employee will be treated as a visitor in accordance with the IT-SEC-0014 Visitor Policy.

4.1.4 Terms & Conditions of Employment

Each user must sign a confidentiality statement that they understand the nature of the information they access, that they will not use the information for unauthorized purposes, and that they will comply with all applicable information technology security policies which includes IT-GEN0002 Asset Disposal Policy and IT-SEC-0006 Media Sanitization policies covering the requirement to return or destroy any information or assets when their employment terminates.

Newly hired employees will not be allowed access to the UF COLLEGE OF PHARMACY facility until the University Of Florida College Of Pharmacy Human Resources Department has issued initial approval of employment.

4.2 Stage 2 Maintenance of User Access

4.2.1 Center Standards for Maintenance

The UF COLLEGE OF PHARMACY Information Security Manager (ISM) must ensure that all users are aware of information security threats and concerns, their responsibilities, and liabilities, and are equipped to support organizational security policy in the course of their work, and to reduce the risk of human error. It is also necessary that user changes in role or business environment are carried out in an orderly manner that ensures the continuing security of the information systems to which they have access.

4.2.2 Management Responsibilities

Managers must notify the UF COLLEGE OF PHARMACY’s IT Helpdesk in a timely manner of any changes in a user’s role or business environment to ensure that the user’s access can be changed as appropriate. Processes must ensure that access to information systems is extended to include new
user requirements and also that any access that is no longer needed is removed. Any changes to user access must be made in a timely manner and be clearly communicated to the user. UF COLLEGE OF PHARMACY managers must require users to understand and be aware of information security threats and their responsibilities in applying appropriate UF COLLEGE OF PHARMACY policies. This requirement must be documented.

These policies include:

- **IT-SEC-0002 Acceptable Use Policy**
- **IT-SEC-0008.001 Data Security Standard**
- **UF Information Privacy Policy – 1.3 – Maintaining Confidentiality of Health Information**

4.2.3 Information Security Awareness and Training

All data users are required to receive appropriate information security awareness training and regular updates in related statute and organizational policies and procedures as relevant for their role. It is the role of managers to ensure that their staff are adequately trained and equipped to carry out their role efficiently and securely.

4.3 Stage 3 Termination of User Access

4.3.1 Secure Termination of Access due to End of Assignment or Employment

Termination of employment may be due to resignation, change of role, suspension, or the end of a contract or project. For all terminations access to UF COLLEGE OF PHARMACY information assets needs to be removed in a timely manner when no longer required by the user.

4.3.2 Termination Process and Responsibilities

Managers must notify the Office Manager and Information Security Manager in a timely manner of the impending role change, termination, or suspension of employment so that their access can be revoked or suspended. UF COLLEGE OF PHARMACY IT Helpdesk must notify the appropriate system owners who must revoke or suspend access for that user at an appropriate time, taking into account the nature of the termination. Responsibilities for notifying changes, performing employment termination, or change of employment must be clearly defined and assigned.

4.3.3 Return of Assets

Processes must be implemented to ensure that users return all of the organization’s assets in their possession upon termination of their employment, contract, or agreement. This must include any copies of information in any format.
Information Technology Department

4.3.4 Removal of Access Rights

Processes must be implemented to ensure that all access rights of users of UF COLLEGE OF PHARMACY information systems shall be removed in a timely manner upon termination or suspension of their employment, contract, or agreement.

Process and responsibilities must be agreed and implemented to enable emergency suspension of a user’s access when that access is considered a risk to the UF COLLEGE OF PHARMACY or its systems as defined in the *University of Florida IT Security Incident Response Procedures, Standards, and Guidelines*.

5.0 Policy Compliance

5.1 Compliance Management

The UF COLLEGE OF PHARMACY Information Security Manager (ISM), or their designee, will verify compliance to this policy through various methods, including but not limited to, periodic walk-thru inspections, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner and privacy committee.

5.2 Exceptions

The UF COLLEGE OF PHARMACY Information Security Manager (ISM), or their designee must approve any exception to the policy in advance.

5.3 Non-Compliance

An employee found to have violated this policy would be subject to disciplinary action, up to and including termination of employment.

6.0 Policy Scope

This policy applies to any person that requires access to UF COLLEGE OF PHARMACY information systems or information of any type or format (paper or electronic).

The policy applies automatically to all UF COLLEGE OF PHARMACY personnel, contractual third parties, and agents of the UF COLLEGE OF PHARMACY.

Where access is to be granted to any third party (e.g. contractors, service providers, partners) compliance with this policy must be agreed and documented. Responsibility for ensuring this lies with the UF COLLEGE OF PHARMACY Information Security Administrator (ISA) prior to issuing this third party access.
Information Technology Department

7.0 Related Policies

- IT-GEN-0002 Asset Disposal Policy
- IT-SEC-0002 Acceptable Use Policy
- IT-SEC-0006 Media Sanitization
- IT-SEC-0008.001 Data Security Standard
- UF Information Privacy Policy – 1.3 – Maintaining Confidentiality of Health Information
- University of Florida IT Security Incident Response Procedures, Standards, and Guidelines

8.0 Definitions

Data Owner
The primary person responsible for the data being utilized by the center. Should be the person ultimately responsible for authorizing access to the data, as well as, provide classification of the data.

Access Period
The period of time during which an UF COLLEGE OF PHARMACY employee, contractual third party, or agent of the UF COLLEGE OF PHARMACY has access to information or information systems of the UF COLLEGE OF PHARMACY.

UF COLLEGE OF PHARMACY IT Helpdesk
The internal UF COLLEGE OF PHARMACY team that handles day to day support of the center and all of its constituents.

UF COLLEGE OF PHARMACY Personnel
All individuals involved in providing medication performance measure services on behalf of the UF COLLEGE OF PHARMACY.

Managers
All individuals within the UF COLLEGE OF PHARMACY that hold any of the Lead, Director, or Faculty position designations. Example: Lead Technician, Lead Clinical Associate, Lead Clinical Pharmacist, Director, Assistant Director.

9.0 Supporting Information

No additional supporting information was provided.