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>10/17/2017</td>
<td>Lane Blanchard</td>
<td>Initial document draft</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 locations that include computers and other types of information technology resources must be safeguarded against unlawful and unauthorized physical intrusion, as well as fire, flood and other physical threats. These safeguards include but are not limited to; security doors, key entry areas, external
doors that are locked from closing until opening of the building, locked and/or barred windows, security cameras, registration of visitors at entrances, and fire protection.

Information Security issues to be considered are:

- Unlawful access may be gained with the intent of theft, damage, or other disruption of operations.
- Unauthorized and illegal access may take place covertly (internal or external source) to steal, damage, or otherwise disrupt operations.
- Destruction or damage of physical space may occur due to environmental threats such as fire, flood, wind, etc.
- Loss of power may result in the loss of data, damage to equipment and disruption of operations.

4.0 Policy Details

4.1 Physical Access Control

4.1.1 Employee Access & Identification

4.1.1.1 New Employees

All new employees must be screened in accordance with IT-SEC-0012 Human Resource Security Policy prior to being granted physical access to any work location. The hiring authority for the new employee, or their designee, must submit an access request specifying the areas the employee will require access to, as well as, a request for picture identification. This request needs to include confirmation that the requirements of employee mandated background screenings have been satisfactorily completed.

4.1.1.2 Current Employees

All employees must have their employee identification displayed prominently on their persons at all times while they are working in an official capacity for the Center. Due to the nature of our environment, all employees must also display the provided Center Staff identification at all times.

Any employee that does not have their employee identification must report to the visitor area, and their supervisor or manager will be notified. If the employee’s supervisor or manager approves, then the employee will be provided a temporary visiting employee badge. This badge will be valid for no more than 12 hours, and repeat offenders will face disciplinary action, up to termination.

It is the responsibility of all employees to ensure that the secure workspace is protected. All employees should challenge anyone within the workspace that does not have appropriate identification and / or escort.
4.1.1.3 Exiting Employees

When an employee leaves the UF COLLEGE OF PHARMACY the supervisor for the employee, or their designee, must submit a request for revocation of access to facilities and information systems. If the employee is exiting voluntarily, the request should be submitted no later than 24 hours prior to the employee’s last day. This request should include a copy of the employee’s resignation letter. If the employee is leaving involuntarily, the request should be completed prior to the employee being notified.

The employee should surrender their employee identification at the end of their final shift to a supervisor. If the employee is also a student of the University of Florida, then they should retain their badge. The supervisor will return any surrendered identification to the UF COLLEGE OF PHARMACY Information Security Administrator (ISM) for proper disposal.

4.1.2 Loss of Employee Identification

In the event that an employee should lose their identification, they are required to notify their manager / supervisor immediately so that access can be removed from the identification. The manager / supervisor should submit a request immediately to have all physical access removed from the employee until they have received new identification or located their lost identification.

It is the responsibility of the employee to get a replacement identification card from the appropriate issuing authority. Once the employee has resolved their identification issue, the manager / supervisor should submit a request for physical access to be granted to the employee.

4.1.3 Visitor Access & Identification to restricted areas

All visitors are to be handled according to IT-SEC-0014 Visitor Policy.

4.1.4 Individual Office Security

Any office that has a lock installed must be locked when the occupant leaves for the day. The lock is present to prevent theft or abuse of the office and its equipment by unauthorized people.

All office locks must have, at minimum, two keys provided for access to the office. One key should be provided to the occupant of the office, and other key(s) should be secured in a lockbox and labeled for access in an emergency. This second key will be issued, per UF policy, to the UF COLLEGE OF PHARMACY Information Security Manager (ISM) or their delegate.
All locking furniture located within each office must have, at minimum, two keys for each different lock for access to its contents. One of each unique key should be provided to the occupant of the office, and other key(s) should be secured in a lockbox and labeled for access in an emergency.

Where a centralized facilities team exists that has master keys / access to all offices, then there will be no need for a lockbox.

All keys that are issued to personnel should follow a process that is in agreement with *IT-GEN-0001 Asset Management Policy*.

4.1.5 Sterile Area Security

The primary entry doors to all sterile areas should be secured using electronic locks that provide auditable logs of entry into the sterile area. These logs should be available for inspection with reasonable notification to ensure that incidents can be properly investigated.

In order to comply with University of Florida safety requirements, each primary entry door should also be secured with a standard key lock as well. This lock should use the restricted master key cylinder to allow University Police & Security personnel access to the area in the event of an electronic lock failure. In addition to the University Policy & Security personnel, master keys will be issued to specific internal personnel as required.

All master keys should be secured in a lockbox and labeled for access in an emergency. In the event that a master key is issued, it should follow a process that is in agreement with *ITGEN-0001 Asset Management Policy*.

4.2 Internal Security Control

4.2.1 Use of Personal Electronics

The use of personal electronics within any area of the UF COLLEGE OF PHARMACY is allowed. This includes, but is not limited to:

- Smartphones, PDAs, and cellular phones
- Personal Laptops
- Digital Cameras, Video Cameras, and other similar recording devices
- Tape Recorders, Digital Recorders, and other similar audio recording devices
- Tablets, e-Readers, and music players

Management and Information Technology team members are included in the above BUT due to the nature of their jobs, but they should take care to avoid using these devices in the sterile area of the College of Pharmacy, for example the CQM Call Center, whenever possible.
4.3 Physical Security Incidents & Reporting

A security incident is defined as any event that could result or has resulted in:

- The integrity of the working process being put at risk.
- The availability of a resource being put at risk.
- An adverse impact, such as:
  - Embarrassment to the University of Florida, College of Pharmacy.
  - Threat to personal safety.
  - Legal obligation or penalty.
  - Financial loss.
  - Disruption of work activities.

All incidents or information indicating a suspected or actual break of physical security must be reported immediately to the UF COLLEGE OF PHARMACY Information Security Manager (ISM). The types of incidents that can result in a breach of physical security are many and varied.

Their severity will depend upon a myriad of factors but the majority will be unintentional and will not normally result in any form of disciplinary action. The likely result will be improved security and awareness throughout the center.

Any member of staff reporting a breach of security will have unhindered access to the UF COLLEGE OF PHARMACY ISM. If that member believes that breach is as a result of an action or negligence on the part of the UF COLLEGE OF PHARMACY ISM, then the member will have direct access to the UF COLLEGE OF PHARMACY Information Security Administrator.

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 addresses threats to critical IT resources that result from unauthorized access to facilities owned or leased by the University of Florida and/or the College of Pharmacy, including offices, data centers and similar facilities that are used to house such resources.

7.0 Related Policies

- IT-SEC-0012 Human Resource Security Policy
- IT-SEC-0014 Visitor Policy

8.0 Definitions

Sterile Area  The protected area(s) of the facility where member contact activities occur and extending to all immediate perimeter walls to include offices, conference rooms, and any other storage area within those immediate perimeter walls.

9.0 Supporting Information

No additional supporting information was provided.