Ellis Human Development Institute
School of Professional Psychology
Wright State University

Cyber Security Policy

I. Purpose

The purpose of this document is to identify the relevant HIPAA and Information Security related policies for the Ellis Institute (Ellis) and provide immediate actions that all Ellis Institute faculty, students, and staff can take that will address the intent of the requirements. This, in turn, will help the Ellis Institute operate in a secure manner, by increasing the security knowledge of its workforce, by taking proactive steps to protect the sensitive data belonging to their clients and ensuring the confidentiality, integrity, and availability of all information in their care.

II. Applicability

The policies and recommendations outlined in this document are applicable to all Ellis Institute faculty, staff, students, and employees that have physical and logical access to Wright State University (WSU) and Ellis Institute information systems, client information, and privacy information. Each procedure will address a specific regulation(s) and provide industry best practices recommendations.

III. Wright State University & Ellis Institute Security Policies and Procedures

All security policy and procedures at the Ellis Institute must be aligned with the WSU “Wright Way” security policies and HIPAA guidelines. Ellis Institute faculty, students, and staff must review the WSU security policies accessible via the below link.

http://policy.wright.edu/policy/11300-it-security-policy
# Table of Contents

   1.1 Passwords ........................................................................................................................................... 3
   1.2 Operating System Updates .................................................................................................................. 4
   1.3 Virus Protection ................................................................................................................................. 4
   1.4 Spy and Malware Protection ............................................................................................................... 5
   1.5 Firewalls ............................................................................................................................................ 5
   1.6 Email .................................................................................................................................................. 6
   1.7 Instant Messaging (IM) ..................................................................................................................... 7
   1.8 Data Integrity ..................................................................................................................................... 8
   1.9 Encryption ......................................................................................................................................... 8
   1.10 Mobile Devices (Phones, Tablets and Laptops) .................................................................................. 9
   1.11 Removable Media ............................................................................................................................. 9

2. Incident Identification and Response ...................................................................................................... 10
   2.1 Breaches and Breach Notification ....................................................................................................... 10
   2.2 Risk Management and Business Continuity Planning ....................................................................... 11
   2.3 Emergency Operations ..................................................................................................................... 11

3. Security Awareness ................................................................................................................................. 12
   3.1 HIPAA ............................................................................................................................................... 12
   3.2 Privacy .............................................................................................................................................. 13
   3.3 OMNIBUS .......................................................................................................................................... 13

4. Physical and Logical Security .................................................................................................................. 14
   4.1 Logical Security ................................................................................................................................. 14
   4.2 Visitors .............................................................................................................................................. 15

Author and Approval .................................................................................................................................... 15

Revision History .......................................................................................................................................... 15
1. Security Best Practices

All employees and users of network computing resources at the Ellis Institute have a role in protecting the institution’s information resources because their computers provide potential gateways to protected information stored on the systems at the Ellis Institute. Therefore, whether or not you deal directly with sensitive information such as Protected Health Information (PHI), Personally Identifiable Information (PII), or electronic PHI (ePHI), you should be fully aware of the security implementations put in place to ensure the security of all information resources.

1.1 Passwords

The Ellis Institute follows the WSU Computing and Telecommunications Services (CaTS) program password policy and complexity standards. Every user is responsible for keeping their password secure. This can be done by following basic security best practices, all of which are designed to protect the authorized user.

i. Create a unique password that uses a combination of letters, numbers, special characters, and symbols.

ii. Do not use your network username as your password.

iii. Do not share your passwords with anyone. CaTS will never ask for your password. If you receive an email purported to be from CaTS requesting your password, it is likely an attempt to gain your credentials by a fraudulent source.

iv. Do not write down passwords or hide under your keyboard – select memorable, strong passwords or pass phrases.

v. Do not use an easily guessed password such as “User” or “Password”.

Ellis Institute Users will:

i. Abide by policies stated in the WSU Computing and Telecommunications (CaTS) Account Policy Statement

ii. Use CAMPUS passwords and user logon IDs

iii. Follow CAMPUS password standards set forth on the WINGS portal: http://wings.wright.edu

iv. Ensure CAMPUS passwords are kept private i.e., not shared, coded into programs, or written down. Users will be held accountable for all actions performed with the use of these credentials.

v. Ensure CAMPUS passwords for faculty and staff are changed every 180 days and Student passwords are changed every 5 years. Systems will enforce password change with an automatic expiration and prevent repeated or reused passwords.

vi. Acknowledge that CAMPUS user accounts will be locked after 9 failed logon attempts and all failed login attempts will be recorded and audited.
1.2 Operating System Updates
Operating System updates are small programs or files that patch operating systems (such as Windows) against known problems. These updates are crucial in defending against new viruses and attacks. Hackers are constantly looking for vulnerabilities in operating systems and programs, and can easily find and infiltrate a computer that has not been properly patched. If for some reason you suspect that your computer has not been properly patched, you should contact the WSU CaTS helpdesk immediately at helpdesk@wright.edu.

For CaTS managed computers on the WSU network (normally defined as faculty, staff, and administrative computers), security updates are automatically installed from our update server. For students living in the residence halls, or home users, your computer should be set up to automatically download and install critical updates. For specific directions on how to do this for your particular operating system, see the Do IT Wright website, located at http://www.wright.edu/security/

All systems connected to the WSU's network must have a vendor supported version of the operating system installed. All systems connected to the WSU's network must be current with security patches.

Ellis Institute users will:

i. Follow all directions received from WSU CaTS regarding operating system patch updates and immediately act on any instructions to apply or verify patches.
ii. Not attempt to make administrative changes to the secure configuration of their assigned workstation or laptop
iii. Contact the WSU CaTS helpdesk should they suspect their workstation or laptop has not been properly patched or updated
iv. Follow WSU and Ellis Incident Identification and Response procedures should they suspect their computer has been compromised

1.3 Virus Protection
A computer virus is a program that implants instructions into your computer programs or storage devices that can then attack, scramble, or erase computer data. The destructiveness of viruses lies in their ability to replicate themselves and spread from system to system. It is very important to have anti-virus software running on your computer and to keep it up-to-date so that new viruses can be detected.

CaTS requires all computers connected to the WSU network have up-to-date anti-virus software. For CaTS supported systems on campus, including Ellis (faculty and staff offices), this is done automatically.

Ellis Institute users will:

i. Adhere to WSUs Anti-Virus software program and not install any program or software that will attempt to circumnavigate or disable the anti-virus protections installed by WSU CaTS.

https://www.wright.edu/information-technology/security/anti-virus-software
ii. Not install their own anti-virus software as it may conflict with the functionality of software already installed

iii. Confirm that anti-virus software is installed on their desktop, laptop or another device when contacted directly by a member of the WSU CaTS team

iv. Not connect any device to the WSU/Ellis network that has not been scanned for viruses by CaTS and/or authorized to connect to the WSU network

v. Follow WSU and Ellis Institute Incident Identification and Response procedures should they suspect their computer has been compromised

1.4 Spy and Malware Protection

Spyware is any software that watches your computing activity and collects personal data without your permission. It can be hidden in programs that you download from the Internet. Once you install that program, the spyware can monitor your activity and send that information to someone else. Email addresses, web browsing habits, usernames, and passwords are just some of the data that spyware can collect.

This data can then be used for identity theft, marketing, spam, and other activities. Along with the ability to steal your information, spyware also consumes large amounts of memory on your computer, making it more unstable and prone to crashing. To reduce the amount of spyware on your computer, all computers connected to the WSU network are required to have actively updated spyware protection software installed if available for that operating system.

Ellis Institute users will:

i. Follow WSUs Anti-Spyware and Anti-Malware program and not install any program or software that will attempt to circumnavigate or disable the protections installed by WSU CaTS

ii. Not install their own anti-spy and anti-malware software as it may conflict with the functionality of software already installed

iii. Not install or attempt to install any unauthorized software or programs on a computer provisioned by WSU CaTS and/or Ellis

iv. Not click on links embedded in emails from unknown or unexpected sources

v. Not save their password on any computer

vi. Never run a program (.exe file) unless authorized to do so

vii. Follow WSU and Ellis Institute Incident Identification and Response procedures should they suspect their computer has been compromised

1.5 Firewalls

A firewall is a system that is designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software formats. At WSU, CaTS maintains both hardware and software perimeter firewalls for the entire campus community that control internet traffic in and out of our network.
For individual computers, personal desktop firewalls, such as Windows Firewall, must be enabled to help prevent unauthorized access.

**Ellis Institute users will**

i. Not attempt to disable any firewall software previously installed by WSU CaTS provisioned computer

ii. Not attempt to access the firewall software to modify it

iii. Contact the WSU CaTS helpdesk should they experience connection issues that may be related to the firewall software

### 1.6 Email

Email is not secure. Never put sensitive information, such as test or evaluation results, Social Security Numbers, PII, ePHI or any other sensitive information into any part of your email or email attachments unless the email and attachment are encrypted. Emails can be encrypted by typing the word “Encrypted” into the subject line.

**It is the policy of the Ellis Human Development Institute to not send client information and private employee/student information via email.**

In addition to following the policy guidance identified by WSU, and a best practices approach to email security, end user education is key in thwarting many of the threats that are focused on the weaknesses within email. Many of the problems with email are technology based and must be dealt with using technical solutions backed up by end user education.

**Ellis Institute users will**

i. Not send attachments containing ePHI or PII

ii. When sending an encrypted message through email, faculty, students and staff will not include the password to unlock the file in an email

iii. Use the WSU spam filter technology (Proofpoint)

   a. [http://www.wright.edu/information-technology/security/anti-spam-service](http://www.wright.edu/information-technology/security/anti-spam-service)

iv. Not forward documents or emails containing institutional data to outside email accounts such as Gmail, Yahoo, I mail or another third party vendor, without first obtaining approval from management and/or the Department of Information Security officials

v. Not share WSU or Ellis email passwords

vi. Not open unsolicited emails or attachments as they may contain malware or other unwanted executable software

vii. Not forward emails that they have received on an outside email account to a WSU or Ellis email account.

viii. Read email scam alerts regarding identified phishing attempts

In addition to the above security guidelines, Ellis faculty, students and staff will be made aware of the following:
i. Forgery (or attempted forgery) of electronic mail messages is prohibited
ii. Attempts to read, delete, copy, or modify the electronic mail of other users are prohibited
iii. Attempts to send harassing, obscene and/or another threatening email to another user are prohibited
iv. Use of electronic mail services for purposes constituting clear conflict of WSU and Ellis interests or in violation of Policy for Responsible Use of Information Technology is expressly prohibited
v. The use of email in any way to facilitate the conduct of a private commercial purpose is prohibited
vi. The contents of email messages will not be considered private and are subject to the Sunshine Laws
vii. Users may not use WSU CaTS mail servers for any purpose prohibited by the WSU / Ellis email use policy or applicable state and federal laws

1.7 Instant Messaging (IM)

Instant messaging software is not a secure form of communication. Information transmitted via these software packages is not encrypted and always travels outside of the university network environment prior to arriving at its destination, even if that destination is another individual at WSU.

Malware attacks focused on IM technology vulnerabilities require that approved IM clients are patched and maintained. WSU and Ellis require that all file transfers be encrypted during the entire process, thus making the use of IM technologies unsuitable for that purpose. Data transmitted via IM technologies that are not encrypted travels across the internet and is potentially visible to eavesdroppers at any point on its internet path from the sender to the receiver.

Ellis Institute users will

i. Not transmit Institutional Data in an instant message or via a file transfer or any other means of communication these programs provide
ii. Not attempt to install or download programs of this type or nature onto WSU/ Ellis provision workstations, laptops or mobile devices.
iii. Adhere by the guidelines and security standards regarding the use of programs such as Instant Messaging

---

1 Sunshine laws are regulations requiring openness in government or business. Sunshine laws make meetings, records, votes, deliberations and other official actions available for public observation, participation and/or inspection. Sunshine laws also require government meetings to be held with sufficient advance notice and at times and places that are convenient and accessible to the public, with exceptions for emergency meetings.

Read more: Sunshine Laws Definition | Investopedia
1.8 Data Integrity
Protecting the integrity of data is another very important step in the overall health of the WSU and Ellis information. You can do this in a number of ways, most notably through using data encryption methods, backing up the data on a regular basis, and using Virtual Private Network (VPN) software when connecting to WSU and Ellis information from remote locations.

For more information concerning CaTS VPN go to:
http://www.wright.edu/sites/default/files/page/attachements/vpn_policy_printable_0.pdf

Ellis Institute users will
i. Review the WSU guidance regarding data integrity
ii. Ensure all data within their purview is properly protected from alteration, modification or deletion
iii. Prior to making any changes to data, confirm with the data owner that the changes have been approved
iv. Prevent unauthorized use of computers by ensuring automatic logoff functionality is working and manually logging off while away
v. Not post passwords publically

1.9 Encryption
Encryption is the process of transforming information from clear or plain text into a non-readable format so that only the intended reader can understand or change the message content. Encryption ensures privacy. It is a way to keep prying eyes from reading confidential information that is sent across the public internet.

Certain software applications have encryption methods embedded in them for sending and receiving secure information and for the storage of information. There is also third party software available that can be used to encrypt information. For directions on encrypting files, check out the "Encryption" area on the following website:
http://www.wright.edu/security/itwright/habits.html#integrity

Ellis Institute users will
i. Review the WSU guidance on data encryption
   a. https://www.wright.edu/information-technology/security/encryption
ii. Implement encryption requirements for all permissible outgoing communications (see email guidance) that contain sensitive information such as PII, PHI, and ePHI.
iii. Synch their Windows password with the provided Full Disk Encryption software provided by WSU
1.10 Mobile Devices (Phones, Tablets, and Laptops)

Information stored on laptop computers, personal organizers (e.g. Blackberry, Palms), cellular phones, thumb drives, and other similar mobile devices is susceptible to equipment failure, damage, or theft. Information transmitted via wireless connections is not always secure—even networks using certain types of encryption are vulnerable to intruders.

Users with access to the electronic health information system (CATT) at the Ellis Institute must install the Duo application on their cell phone. Ellis Institute users must first use this application as part of a two-factor authentication process to log-in to CATT via a trusted computer workstation.

Ellis Institute users will

i. Password protect mobile devices approved for use and enable the auto-lock function
ii. Adhere to standard security protocols, such as patching the O/S and installing application updates to personal devices
iii. Encrypt documents containing sensitive information before they are placed on portable devices unless the entire drive or data storage of the device is encrypted (WSU policy)
iv. Have smartphones capable of receiving and sending email configured to connect to the WSU or Ellis email server via secure IMAP Post Office Protocol (POP) is not to be used
v. Protect and secure mobile devices from theft and unauthorized viewing of client information at all times
vi. Use CaTS VPN when transmitting sensitive information via wireless technologies
vii. Use personal firewalls on laptops that will access the WSU Network from a remote location
viii. Immediately report any loss or theft of a mobile device containing sensitive information to the Department of Information Security
ix. Backup the data on your mobile devices on a regular basis—backup media should be stored in a secure location or the backup should be encrypted
x. Disable Bluetooth wireless to protect mobile devices from unauthorized access

1.11 Removable Media

The Ellis Institute does not allow the use of removable media (CDs, DVDs, flash drives or portable hard drives) to store or transmit sensitive client data. Ellis Institute faculty, students, and staff are not permitted to transfer files from the surveillance system to any removable media for later use.
2. Incident Identification and Response

WSU has developed incident response guidance that should be applied to all computer security incidents at WSU. This guidance also applies to Ellis and should be reviewed by all Ellis faculty, students and staff to ensure a seamless approach to the handling of incidents, including computer security incidents and data breaches.

The Office of Information Security will oversee information security incident handling in cooperation with designated Technical Managers, Office of General Counsel, University Police Department, Office of Student Affairs (only where students are involved), and other designated support staff. Any person who receives notification of or discovers an information security incident must contact the Office of Information Security and responsible IT department personnel and file an incident report prior to taking any action.

Ellis Institute users will

i. Review all guidance provided by WSU regarding Computer Security Incidents
   a. The WSU Computer Incident Response and Management Plan discusses in detail what an incident looks like and how it should be responded to:
      Computer Incident Response and Management Plan (PDF)
   b. Incident Handling and Notification Procedures:
      http://www.wright.edu/information-technology/security/report-a-security-incident
   c. WSU Incident Response Form:
      https://webapp2.wright.edu/cats/security/incident.php

2.1 Breaches and Breach Notification

Following a review of the WSU Computer Incident Response and Management Plan as well as the Incident Handling and Notification Procedures, all Ellis Institute users should have a clear understanding of what constitutes a computer security incident, which may also be identified as a “breach”. A breach, or data breach, constitutes more than the possibility of malware being installed on a computer or a system being hacked or a password being stolen. A data breach is an incident in which sensitive and/or protected data has been viewed, stolen or used by an unauthorized person.

In all cases involving a computer security incident, the Incident Response Plan (IRP) may be referred to for guidance on how to identify the type and severity of the incident. The IRP may also be used as guidance on how and when to notify those persons or organizations impacted by the suspected data breach. In most cases, the initial notification process takes place immediately following the detection of a breach and should consist of a pre-planned message to those affected.

In the event of a suspected data breach, Ellis Institute users will:

i. Refer to the WSU Incident Handling and Notification Procedures
ii. Inform their immediate supervisor at the Ellis Institute regarding a suspected breach
iii. Conduct a physical inventory of all sensitive data in their immediate care, including electronic records that may be stored on their WSU assigned computer or laptop (if allowed)
iv. Refrain from any further communication regarding the incident and/or status of the incident
In the case of a breach involving PHI, WSU’s privacy officer will be responsible for notice to individuals and will include:

a. Affected individuals must be notified following the discovery of a breach
b. The notice must be provided in written form by first-class mail, or email if the affected individual has agreed to receive electronic notices.
c. Through a substitute contact if the affected individual’s contact information is out-of-date
d. A toll-free phone number must be provided to affected individuals and remain active for at least 90 days
e. Notifications must be provided without reasonable delay, no later than 60 days following the discovery of a breach and must include a brief description of the incident

Additional, in-depth guidance regarding breaches can be found at:

http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Ellis Institute administration will work with the WSU incident response team to test the incident response readiness capabilities of the Ellis Institute to ensure incidents/breaches are handled in a timely manner and in accordance with specified policy from WSU and HIPAA (OMNIBUS).

2.2 Risk Management and Business Continuity Planning

WSU and the Ellis Institute maintain an active Risk Management Program and conduct business continuity tests and exercises of that program on an annual basis. The Ellis Institute will conduct a risk assessment annually to identify and mitigate risks to PHI and ePHI. Ellis Institute administration will participate with the Computing and Telecommunications Services (CaTS) information security office in the annual WSU exercise. The Ellis Institute will follow the risk management policies and procedures defined by WSU, in addition to its own Business Continuity Plan, to ensure a seamless organizational approach to risk management and business continuity planning.

2.3 Emergency Operations

WSU has developed a comprehensive emergency notification system with the sole purpose of keeping faculty, students and employees informed about emergencies and life-threatening situations on campus. All Ellis Institute personnel have the capability of being notified of an emergency situation via the following communication formats:

- Email: all @wright.edu email addresses are automatically enrolled in Wright State Alert!
- Text message
- WSU Homepage
- Voice phone message
- Twitter
- Facebook

The Ellis Institute will implement the emergency procedures developed by WSU and follow all applicable guidance regarding emergency conditions. All emergency procedures for WSU can be found at:
In addition to these WSU emergency procedures, personnel assigned to the Ellis Institute will follow procedures described in its Emergency Management Plan whenever an emergency situation occurs within the confines of the Ellis Institute.

3. Security Awareness
WSU has prepared a series of security awareness training presentations that all Ellis Institute faculty, students, and staff must review prior to gaining full access to WSU and Ellis Institute information systems and resources. Ellis Institute users should review this material on an annual basis or when any significant changes occur within the WSU and Ellis Institute Security Awareness program(s).

Ellis Institute users will

i. Review the training material and information
ii. Upon completion of relevant training, generate evidence proving that they have completed the training material
iii. If a completion signature page is provided, print and save it for future reference
iv. Submit the signature page to your immediate supervisor if required

The CaTS security training includes the following:

i. Introduction to Computer Security:
   http://www.wright.edu/sites/default/files/page/attachements/intro_to_security_0.pdf
ii. WSU Security Awareness Guide:
   http://www.wright.edu/sites/default/files/page/attachements/security_companion_guide_1.pdf

3.1 HIPAA
The Health Insurance Portability and Accountability Act (HIPAA) regulates the protection of private health information for individuals. HIPAA requires an individual's medical records and other protected health information be safeguarded and kept confidential. HIPAA-related data must be available to only those with sanctioned access and be encrypted when transmitted electronically. For more information on HIPAA, see WSU's HIPAA Privacy Manual and HIPAA Security Awareness Training Module.

The WSU Privacy Officer has created a HIPAA Training presentation that all Ellis Institute users must review prior to being granted full access to HIPAA-related data.
The HIPAA Security Awareness Training Module can be found at: [http://www.wright.edu/information-technology/security/security-training](http://www.wright.edu/information-technology/security/security-training)

### 3.2 Privacy

The Ellis Institute is required to follow the privacy policy requirements outlined by WSU. Additionally, due to the nature of information used at the Ellis Institute, there is a requirement to be compliant with the privacy and security protections identified in the HIPAA and subsequent OMNIBUS regulations. The HIPAA/OMNIBUS regulations call for the use of appropriate safeguards to protect the privacy of PHI and establish predetermined conditions on the use and disclosures that can be made without the authorization of the client. Lastly, the HIPAA Privacy Rule(s) address client rights in regard to examining and obtaining a copy of their records to request corrections.

**Ellis Institute users will**

i. Guard against improper disclosure of PHI, PII or ePHI
ii. Not disclose privacy information without proper approvals and/or authorizations
iii. Protect the privacy information of minors and/or the decedent
iv. Comply with guidelines regarding the disclosure of information to law enforcement, government agencies, family and/or friends
v. Maintain the confidentiality of information in their care

[https://www.wright.edu/about/privacy-policy](https://www.wright.edu/about/privacy-policy)

### 3.3 OMNIBUS

The HIPAA OMNIBUS Rule addresses four specific areas within the HIPAA guidance. These four areas address the following:

1. HIPAA Privacy, Security, and Enforcement Rules mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act, and certain other modifications to improve the Rules
2. HIPAA Enforcement Rule to incorporate the increased and tiered civil money penalty structure provided by the HITECH Act
3. Final rule on Breach Notification for Unsecured Protected Health Information under the HITECH Act
4. Final rule modifying the HIPAA Privacy Rule as required by the Genetic Information Nondiscrimination Act (GINA) to prohibit most health plans from using or disclosing genetic information for underwriting purposes


**Ellis Institute users will:**

i. Adhere to the HIPAA OMNIBUS regulations specific to the protection of privacy information maintained by the Ellis Institute.
ii. Contact the WSU Privacy Officer for clarification of any HIPAA OMNIBUS rulings that may be unclear.

4. Physical and Logical Security

WSU provides badges for all personnel at the Ellis Institute. These badges are for identification purposes only and are not associated with a physical security or access control program. Physical security at the Ellis Institute is, therefore, the responsibility of all personnel.

Ellis Institute personnel will:

i. Complete security awareness training
ii. Display their WSU identification badge at all times
iii. Escort all visitors
iv. Monitor access to restricted areas
v. Be aware of who is in their secure area prior to accessing sensitive information
vi. Properly protect assigned equipment and information
vii. Secure sensitive information when no longer in use
viii. Secure portable equipment in a locked drawer or cabinet when no longer in use
ix. Maintain physical control over sensitive information and return files to the records room immediately when no longer needed for official purposes
x. Not make copies or scan client records and files unless they have the appropriate authority to do so
xi. Not share passwords or access codes to secure areas
xii. Close and lock doors to rooms that may contain sensitive information and equipment when not in use

4.1 Logical Security

Logical access controls are in place to ensure users with authorized access to WSU and Ellis Institute information systems and resources have only the minimum level of access required to perform their assigned duties.

The WSU IT Security team (CaTS) ensures all workstations require users with authorized access to enter a user ID and password prior to gaining access. All systems are configured to implement access controls to prevent unauthorized persons from gaining access to Ellis Institute information systems and resources. To ensure Ellis Institute systems are properly protected from unauthorized access,

Ellis Institute users will:

i. Not attempt to elevate their assigned access permissions
ii. Not send unencrypted data via email or other electronic formats
iii. Not access untrusted internet sites
iv. Not attempt to install software on their assigned equipment or plug unauthorized hardware into open ports within the facility
v. Change their passwords on a regular basis
vi. Not share their passwords with other users
4.2 Visitors

A visitor is defined as a person who visits the Ellis Institute facility on a temporary basis and is not employed by the Ellis Institute or WSU. Visitors are not allowed unescorted access to the physically secure location(s) within the Ellis Institute.

Ellis Institute personnel will:

i. Monitor/escort visitors at all times
ii. Ensure all visitors have signed in at the front desk prior to leaving the waiting room area
iii. Secure all sensitive information, preventing both visual and/or physical access to that information by a visitor
iv. Upon completion of the visit, ensure the visitor has signed out at the front desk and left the facility

Author and Approval

<table>
<thead>
<tr>
<th>Author:</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mary Jane Kocian-Figueroa (via SecureState)</td>
<td>10/19/16</td>
</tr>
</tbody>
</table>

Revised by: June 22, 2017