Index of FCIM Security and Privacy Policies

Florida College of Integrative Medicine

Security and Privacy Policies

Dated: January 1, 2018

Table of Contents

I. Purpose

The Florida College of Integrative Medicine ("**College**"), which uphold the College's absolute commitment to ensuring open discourse and the free expression of viewpoints and beliefs, must meet legal, contractual, or enterprise confidentiality and security requirements (collectively the "**Security Obligations**") when conducting research and performing services involving Restricted Information and data. The College has adopted a security and privacy framework, including cyber security policies (the "**Security Policies**") and privacy policies for handling personal information (the "**Privacy Policies**" and, together with the Security Policies, the "**Security and Privacy Policies**"), to address regulatory and contractual requirements typical for protecting sensitive data. This framework (a) supports the College's core mission to offering higher education of the highest caliber and integrity, and (b) commits the College to secure information in a manner that reduces risk and complies with its Privacy and Security Obligations.

II. Definitions

Capitalized terms defined in this section are used throughout the Security and Privacy Policies. As indicated, specific terms are given explicit meaning in the context of the College.

Chief Information Security Officer (CISO)
The senior-level College executive or official responsible for establishing and maintaining the enterprise vision, strategy and program to ensure information assets and technologies are adequately protected. The CISO is the leader of the College's IT Security Office.

Covered Individual
As defined in Section III below.

Departments/Units and Respective Department/Unit Leaders
Admissions Department: Admissions Representative
Assessment Department: Director of Assessment
Finance Department: Director of Finance
Financial Aid Department: Director of Financial Aid
Student Services: Director of Student Services
Clinic: Clinic Director
Dean's Office: Academic Dean
Office of the General Counsel: General Counsel

Designated Secure Storage Facility
Data Centers, Server Rooms, Data Closets and any other secure facility that meets the Physical and Environmental Security Policy controls.

Electronic Media
Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card. Examples include USB flash drives, CDs/DVDs, external hard drives and internal hard drives.

Encryption

The process by which data are converted into secret and unreadable values. To read encrypted data, a person must have access to a secret key or password that enables them to decrypt the data.

Endpoint
Any desktop or laptop computer (e.g., Windows, Apple, and Linux/Unix), Mobile Device or other portable device used to access the College's Information Resources from any local or remote location or access any Information System either owned by the College or by an individual and used for the College's purposes.

Executive Management or Executive Managers
The College's President and Vice Presidents

Information Assets
Servers, endpoints, storage, network and storage switches, firewalls, physical racks containing these, and related software that are components of Information Systems.

Information Owners
Employees who are responsible for classifying Information and protecting the Information according to its Security Obligations. An Information Owner is a steward of data.

Information System
Server based software that resides on a single Server or multiple Servers and is used for business purposes. "Application" or "Information System" is synonymous with "System". E.g. a database server, web server or other application server.

Information System Owners
Employees who have the ultimate responsibility over a particular Information System.

IT Custodians
Employees and/or vetted third party service providers who are technical administrators of the College's Information Systems and Information Assets.

IT Security Office
The department within the College's Administration that is tasked with overseeing the College's overall IT security and is led by the CISO.

Mobile Device
A portable, wireless computing device that is small enough to be used while held in the hand. Some examples of mobile devices include, but are not limited to, smart phones, tablets, and personal digital assistants (PDA), but do not include laptops.)

Privacy Officer
The senior-level executive within the College responsible for establishing and maintaining the enterprise vision, strategy and program to ensure Protected Health Information and other Health Information are protected pursuant to state and federal law, including, without limitation,

HIPAA. All Privacy Officers report to the CISO on matters covered by these Security and Privacy Policies.

Restricted Information
Defined in the College's Data Classification Guideline, referenced above.

Security Incident
Security incident means the attempted or successful unauthorized access, use, Disclosure, modification, or destruction of information or interference with system operations in an information system.

Security Obligations
The applicable regulations and legal, contractual, confidentiality, and security requirements as well as applicable industry standards that the College is obligated to meet.

III. Scope

This policy applies to employees of the College and any other person with access to the College's Information Systems and/or Information Assets ("**Covered Individuals**").

IV. Policy

This policy a) defines the appropriate roles and responsibilities of the College's management and Covered Individuals and b) sets forth the framework the College has implemented to comply with the Security and Privacy Policies and its Privacy and Security Obligations.

IV.A Management Commitment

Executive Management is responsible for overseeing the cyber security efforts for the College. Operational cyber security responsibilities and accountability have been delegated to the College's Chief Information Security Officer (CISO). Operational privacy responsibilities and accountability has been delegated to the Privacy Officer. Where appropriate, Executive Management expects the CISO and Privacy Officer to seek guidance from leadership of relevant departments, the College's Office of General Counsel, and experts within the security and privacy industries when performing their duties.

IV.B Roles and Responsibilities

IV.B.1. Management

Executive Managers represent the interests of their respective supervised departments with respect to the College and provide high-level guidance and direction for the College's security and privacy programs. Their responsibilities include, but are not limited to:

a. Approving the Security and Privacy Policies and associated procedures;
b. Evaluating results of cyber risk analyses and the potential for incidental or unauthorized disclosure of Restricted Information and making risk based decisions for the College; and
c. Commitment to fund the [College's] security and privacy program.

Department and Unit Leaders are responsible for overseeing privacy and cyber security programs within their respective areas of responsibility. Their responsibilities include but are not limited to:

a. Responding to remediation efforts necessary to manage cyber security risks; and
b. Ensuring that each Information System Owner and Information Owner receives security and privacy training.

IV.B.2. Cyber Security Management

The **Chief Information Security Officer (CISO)** is the most senior individual responsible for cyber security at the College. The CISO creates the cyber security strategy as well as day-to-day management of the cyber security program. The CISO leads an Information Security Office, which is a group of information security professionals responsible for carrying out the security program. Executive Managers have delegated to the CISO the sole authority to conduct the following activities within the College. The CISO may delegate these activities to others:

a. Develop, submit to Executive Management for review and approval, disseminate, and assist in the implementation of the Security Policies
b. Assess security risks to Information Systems in partnership with Information Owners and Information System Owners
c. Educate and train Covered Individuals on the Security Obligations, the Security Policies, and relevant security matters
d. Collaborate with the Office of General Counsel and IT Custodians for strategic, tactical, incident management and enforcement actions
e. Seek guidance from and collaborate with the Office of General Counsel to ensure a proper understanding and interpretation of the College's Security Obligations
f. Develop the technical requirements, standards, and guidelines necessary to implement these Security Policies and procedures
g. Grant and document exceptions to any Security Policy
h. Facilitate security incident response and recovery
i. Monitor communications and Information on the College's networks and Information Systems in a manner consistent with The College Policy on Information Technology Use and Access
j. Conduct vulnerability scanning of any Information Asset connected to the College's network or third party Information Systems where permitted by the third party
k. Conduct security assessments of Information Systems and Designated Secure Computing Facilities
l. Disconnect from the College network Information Assets that present a security risk
m. In certain circumstances, as part of managing a response to a security incident, in the expert judgment of the CISO, erase all Information stored on Information Assets used for business purposes, regardless of their ownership.

IV.B.3. Privacy Management

The **Privacy Officer** is responsible for the implementation of and, in consultation with the College's Office of General Counsel, interpretation and application of the Privacy Policies. Specific responsibilities include, but are not limited to:

a. Supervising the appropriate receipt and use of Restricted Information, including Protected Heath Information, in accordance with the Privacy Policies and all Privacy Obligations
b. Providing training on a recurring basis for all Covered Individuals on the Privacy Policies and any other applicable College policies and procedures regarding the privacy of Restricted Information, as necessary and appropriate for such Covered Individuals to carry out their duties
c. Periodically report to Executive Management regarding the status of the College's privacy program
d. Serve as a resource to all Covered Individuals regarding matters related to accessing Restricted Information
e. Investigate and document incident reports
f. Coordinate with other departments within the College and with federal or state auditors, compliance investigators or regulating bodies as needed

IV.B.4. Information Owners

Information Owners ensure compliance with the Security and Privacy Policies in regard to the use of Restricted Information for which they have responsibility. Information Owners will work in conjunction with the CISO and Privacy Officer to understand their Security and Privacy Obligations and to ensure safeguards are implemented in accordance with the Security and Privacy Policies.

IV.B.5. Information System Owners

An **Information System Owner** is responsible for complying with Security Policies with regard to the Information Systems they control. Information System Owners will work in conjunction with the CISO to ensure safeguards are implemented in accordance with the Security Policies. Such responsibilities include but are not limited to:

a. Working with their IT Custodians to ensure proper safeguards are in place to address Security Obligations of the Information System
b. Ensuring that Users and IT Custodians are informed of and abide by relevant Security Policies and procedures

IV.B.6. Information Technology Custodians

An **Information Technology (IT) Custodian** provides technical administration of the Information Assets used by the College. IT Custodians are responsible for ensuring that proper safeguards are in place to address the Security Obligations of Information Assets. They will create, implement and execute technical procedures that meet the Security Obligations applicable to such Information Assets.

IV.B.7. Users

Users are Covered Individuals who are authorized to use College Information and/or Information Assets in the course of their work for the College. Users are expected to comply with the Security and Privacy Policies.

IV.C Organizational Commitment

The Security Policies provide the framework for the College's compliance with its Security Obligations.

The administrative safeguards: The Security Policies and programs are designed to prevent, detect, contain and correct security violations.

The physical safeguards: The Security Policies are designed to (a) limit physical access to the College's electronic Information Systems and Designated Secure Computing Facilities (e.g. data centers) in which they are housed, while ensuring that properly authorized access is allowed, and (b) specify the proper functions to be performed, the manner in which those functions are performed, and the physical attributes of the surroundings of a specific Endpoint or class of Endpoint that can access Restricted Information, and (c) implement physical safeguards for all Endpoints that access Restricted Information to restrict access to authorized users, and (d) manage the receipt and removal of hardware and Electronic Media that contain Restricted Information into and out of a facility, and the movement of these items within the facility.

The technical safeguards: The Security Policies require Information System Owners to implement (a) technical procedures for Information Systems that maintain Restricted Information to allow access only to those Covered Individuals or software programs that have been granted access, and (b) hardware, software, and/or procedural mechanisms that record and examine activity in Information Systems that contain or use Restricted Information, and (c) procedures to protect Restricted Information from improper alteration or destruction, and (d) policies and procedures that verify the veracity of the identify of a person or entity seeking access to Restricted Information.

IV.D Documentation Management

The Security and Privacy Policies are the documented policies, procedures, and controls implemented by College to protect the privacy, security, integrity, and access of Information and Information Assets. The CISO is responsible for creating, reviewing, and revising the Security and Privacy Policies, in consultation with the College's Office of General Counsel.

The College's Office of General Counsel is responsible for creating, reviewing, and revising the Security and Privacy Policies.

All Security and Privacy Policies will be reviewed with a frequency to ensure that they reflect leading practices, no less than every three years, and whenever there is a substantive change to any applicable federal, state, and local regulations impacting the policy.

Standards are defined security rules that apply to Information and/or Information Assets to which Covered Individuals must comply. The CISO is responsible for creating, reviewing, and revising

standards. All standards specific to College are approved by the College's Supervisory Board and/or Executive Management, as appropriate.

Technical procedures are technical steps that Covered Individuals will follow to further implement the Security Policies, procedures and standards. Technical procedures are local, meaning they apply to particular Information System or Information Asset environments. Information System Owners and IT Custodians are responsible for creating, reviewing, and revising technical procedures, in consultation with the CISO.

IV.E Privacy and Cyber Security Governance

The College will review all Security and Privacy Procedures proposed for the College and work with the CISO, Privacy Officer, and the College's Office of General Counsel, as appropriate, to suggest revisions or rewrites thereto. The College will recommend adoption of Security and Privacy Procedures to the Executive Management, which is responsible for final review and approval of the College's Security and Privacy Procedures. Notwithstanding the foregoing, the College's Supervisory Board may, from time to time, adopt immaterial changes to the Security and Privacy Procedures and notify Executive Management of such changes.

IV.F Policy Structure

The Security Policies are in turn a representation of NIST 800-171, itself a selection of controls defined in NIST 800-53r4. These constitute an appropriate framework to meet Security Obligations, including the HIPAA Security Rules, for all activities of the College. Each Security Policy sets forth the purpose, scope, policy, procedures, and risk based controls applicable to the topic covered. Risk based controls are organized in three categories; Core (C), Low (L) and Moderate (M). Risk based controls are determined based on the impact analysis procedure conducted by the Information System Owner.

Category	Description
Core (C)	Controls mandatory and required across the operating environment
Low (L)	Controls as defined by the impact analysis and subsequent risk analysis with the resulting designation of "Low"
Moderate (M)	Controls as defined by the impact analysis and subsequent risk analysis with the resulting designation of "Moderate"

Information Systems designated as a "FISMA Low" must comply with Low controls, in addition to the Core controls. Information Systems designated as a "FISMA Moderate" must comply with Moderate controls, in addition to the Low and Core controls.

V. Exceptions

If any Covered Individual determines he/she cannot follow a Security or Privacy Policy, then they may make a formal policy exception request to the College's Executive Management, who will review the request with the CISO and the Privacy Officer. Only the CISO or Office of General Counsel can grant exceptions to these Securities and Privacy Policies.

VI. Enforcement

The CISO and the College's Office of General Counsel are responsible for interpretation, implementation, and revision of this policy. To the extent there are conflicting interpretations of this policy and another administrative policy, the more restrictive will apply.

A violation of the Security and Privacy Policies may result in corrective actions pursuant to the College's Administrative Policies and Procedures. Corrective actions may include: (a) the immediate suspension of computer accounts and network access; (b) mandatory attendance of additional training; (c) a letter to the individual's personnel or student file; (d) administrative leave without pay; or (e) termination of employment or non-renewal of faculty appointment or student status. Federal and state government agencies have enforcement powers over individuals who violate the law, which can include civil penalties, civil actions, and criminal prosecution.

VII. Applicable Laws, Regulations and Industry Standards

The security and data privacy policies are intended to comply with federal and state laws, including Florida laws, and industry standards that apply to Information Systems and Information Assets.

VIII. Interpretation, Implementation and Revision

The Executive Management of the College, in consultation with the Office of General Counsel and the CISO, is responsible for the interpretation and implementation of the Security and Privacy Policies at the College. To the extent there is a conflict between these policies and another administrative policy, the more restrictive will apply.

Policies and Procedures for Handling Personal Information

I. **Purpose**. These policies and procedures (these "*Policies*") are elements of the College's Security and Privacy Policies and govern the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, and disclosure ("*Processing*") of certain personal information in connection with specified College activities. They apply to all activities of the College (each an "*Activity*"). All College employees, volunteers, trainees, students, and others under the direct control of the College involved in the Activity ("*College Personnel*") are expected to read, understand, and comply with these Policies.

II. **General Administrative Policies**.

a. Privacy Officer. Each Activity will designate a College employee as the Privacy Officer for the Activity. The Privacy Officer is responsible for the implementation of and, in consultation with the College's Office of General Counsel, interpretation and application of these Policies for the Activity. The Privacy Officer is also responsible for receiving complaints and providing further information about these Policies and the Activity's practices relating to information privacy. The designation of the Privacy Officer must be in writing and signed by an authorized College signatory.

In the event a person resigns as Privacy Officer or otherwise ceases to be the Privacy Officer, the Activity will promptly designate a new Privacy Officer. Any Activity that does not have a Privacy Officer is not in compliance with these Policies.

The department, division, or unit in which the Activity takes place will maintain a written or electronic record of each designated Privacy Officer for at least six (6) years from the date upon which such person ceases to be the Privacy Officer.

Unless otherwise specifically designated, each head of department within the College, including but not limited to finance, financial aid, admissions, student services, registrar, faculty and clinic, shall be the Privacy Officer of his/her respective department.

b. Training. The Privacy Officer is responsible for providing training to relevant College Personnel on these Policies and any other applicable College policies and procedures regarding the privacy and security of Personal Information, as necessary and appropriate for such College Personnel to carry out their duties in accordance with applicable Privacy Laws. The Privacy Officer or his or her designee will provide such training on an annual basis, and to new College Personnel when hired or engaged. College Personnel should not attempt to access any Personal Information before receiving such training. College Personnel should also not permit any other College Personnel to access any Personal Information before receiving such training.

The College also provides training to relevant College Personnel whose functions are affected by a material change in privacy or security policies and procedures within a reasonable amount of time after the effective date of the change. The Privacy Officer is responsible for documenting the time, date, place, and content of each training session, as well as the College Personnel who attended each training session. The department,

division, or unit in which the Activity takes place will maintain such documentation for no less than six (6) years from the date of the training and make it available for inspection by regulatory authorities, as appropriate. The Privacy Officer, in consultation with the College's Office of General Counsel, is responsible for determining which individuals must receive the training required by this section.

III. **Handling of Personal Information**.

a. Definition of Personal Information. For the purposes of these Policies, "*Personal Information*" means non-public information about a person that, if disclosed, could reasonably be expected to place the person at risk of criminal or civil liability, or damage the person's financial standing, employability, privacy or reputation and includes, without limitation, the following data types:

   i. Payment Card Industry Information;

   ii. Private Personal Information;

   iii. Protected Health Information;

   iv. Sensitive Identifiable Human Subject Research;

   v. Student Education Records.

b. Use of Personal Information by the College. College Personnel will only collect, record, store, modify, use, and disclose Personal Information as expressly authorized or specifically required in the course of performing their specific job duties. Subject to the foregoing, College Personnel, as directed by the College, may collect, record, store, modify, use, and disclose Personal Information: (1) pursuant to a valid consent or authorization (or valid waiver thereof) from the person to whom such Personal Information pertains (the "*Data Subject*") as long as such activities are not prohibited by law; or (2) as required by law or regulation, as determined by the College's Office of General Counsel.

   Without limiting the foregoing, in the event the College has received Personal Information from a person or entity other than a Data Subject pursuant to the terms of an agreement between the College and the provider of such Personal Information (a "*Data Use Agreement*"), College Personnel may also only use such Personal Information as permitted by the terms of the Data Use Agreement, *unless* otherwise required by law or regulation, as determined by the College's Office of General Counsel.

c. Access to and Use of Personal Information by College Personnel. The standards for the protection of personal information set forth in these Policies are in addition to, and not in lieu of, any other College policies. All College Personnel involved in an Activity, regardless of whether they are College employees, are expected to read, understand, and comply with the standards set forth in that policy when handling Personal Information.

d. Sale of Personal Information and Use for Marketing Purposes. Neither the College, nor any College Personnel, will sell or attempt to sell any Personal Information collected or received as part of the Activity or use any such Personal Information for marketing, fundraising, or other development purposes. For the purposes of these Policies, marketing means making a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

e. Reasonable Safeguards. The Privacy Officer, together with the CISO and any College Personnel who are responsible for safeguarding Personal Information, are expected to implement reasonable technical, administrative, and physical safeguards to protect against uses and disclosures of Personal Information that are not permitted by law or these Policies. Such safeguards will be consistent with any applicable College security or information protection policies. The Privacy Officer, together with the CISO and any College Personnel who are responsible for safeguarding Personal Information, are also expected to use reasonable technical, administrative, and physical safeguards and other reasonable measures to limit incidental uses and disclosures of Personal Information. Incidental uses and disclosures occur as a by-product of another permissible or required use or disclosure that cannot be reasonably prevented through the use of reasonable administrative, technical, and physical safeguards and are limited in nature. For example, an incidental disclosure might involve a visitor overhearing a confidential conversation or glimpsing Personal Information on a sheet of paper carried by a College worker. While these incidental disclosures may occur as a natural consequence of performing the Activity, College Personnel are expected to use reasonable safeguards to prevent them, including: (i) avoiding conversations about Personal Information in front of or around those who do not have the right to access the Personal Information, (ii) lowering voices when discussing Personal Information on the phone or in a room with others; (iii) avoiding using names or other identifying information when discussing individuals in hallways, elevators, or other public spaces; (iv) isolating, locking, or otherwise limiting physical access to file cabinets that contain Personal Information; (v) providing additional security, like passwords, on computers and data repositories that contain Personal Information; and (vi) taking caution when transmitting data that may include Personal Information. All College Personnel are expected to comply with and not attempt to circumvent such safeguards. College Personnel should proactively inform themselves of such safeguards and any relevant security policies by speaking with their supervisors or the CISO.

IV. Special Policies and Procedures for Working with Protected Health Information

a. General. Individually identifiable health and medical information is a special category of Personal Information. Given the particularly sensitive nature of this information, it is often subject to heightened legal and regulatory requirements, including those set forth in HIPAA. In addition to the policies set forth in this document applicable to Personal Information more generally, when working with individually identifiable health and medical information, the policies in this section will also apply. If there is a conflict between the policies in this section and the policies elsewhere in this document or

another College policy, the policy with the more stringent requirements will apply.

b. Identification of Protected Health Information ("*PHI*"). If any College Personnel expect to receive or access any health or medical information, they must promptly, and prior to such receipt or access, contact the Privacy Officer. The Privacy Officer, in consultation with the College's Office of General Counsel, will determine whether such health or medical information constitutes PHI under HIPAA and what contractual or other arrangements are appropriate under the circumstances.

c. Minimum Necessary Standard for PHI. College Personnel will use reasonable efforts to limit their use and disclosure of, and requests for, PHI to the minimum amount necessary to accomplish the purpose of the use, disclose, or request, *except for*: (1) use or disclosure pursuant to a valid patient authorization, in which case the extent of the use or disclosure will be consistent with the scope of such authorization; (2) disclosures to the Director, Office for Civil Rights of the U.S. Department of Health and Human Services (*HHS*) for HIPAA compliance purposes, as determined by the College's Office of General Counsel; (3) disclosures requested by a Covered Entity, such as a health care provider or health plan, with respect to PHI provided to the College by such Covered Entity, in which case the College Personnel may rely upon such request as the minimum amount of PHI necessary for the applicable purpose (if reliance is reasonable under the circumstances); and (4) disclosures required by law, including HIPAA, as determined by the College's Office of General Counsel.

   The Privacy Officer is responsible for identifying persons or classes of persons who need access to PHI to carry out their duties, the categories of PHI to which such persons or classes of persons need access, and any conditions applicable to such access. College Personnel responsible for safeguarding or providing access to PHI will make reasonable efforts to limit access to PHI to only those individuals and categories identified by the Privacy Officer. If any College Personnel receives a request to access PHI from a person who has not been approved to access such PHI, such College Personnel will promptly, and in any event before providing such access, contact the Privacy Officer who will review the request and determine whether the request should be granted.

d. Individual Rights. HIPAA and other federal and state laws provide patients and their Personal Representatives with certain rights to access, amend, and understand the disclosures of their PHI. When patients and Personal Representatives seek to exercise such rights, the College cooperates with Covered Entities that have a direct relationship with such patients.

   Any College Personnel that receive a request for an accounting of disclosures of any PHI, copies of any PHI, or amendment of PHI will promptly, and in any event before responding to such request, forward such request to the Privacy Officer who will consult with the College's Office of General Counsel regarding such request. No College Personnel will respond to, or direct any other person to respond to, such request without the approval of the Privacy Officer and the College's Office of General Counsel. When responding to such a request from the applicable Covered Entity, the College will

respond within the sooner of any time period set forth in the applicable Data Provider Agreement and the following: (i) with respect to requests for accountings of disclosures for the purpose of responding to a patient request, thirty (30) days from the date on which the College receives such request; or (ii) with respect to requests for access to, inspection of, or copies of PHI, or a request to amend PHI, in each case for the purpose of responding to a patient request, twenty (20) days from the date on which the College receives such request.

The department, division, or unit in which the Activity takes place will retain records of each request, referral, accounting, and disclosure of PHI that it receives or creates in accordance with these Policies for a period of at least six (6) years from the date of its receipt or creation.

e. Disclosures Required by Law. If any College Personnel believes that any disclosure of PHI is required by law, such College Personnel must promptly contact the Privacy Officer, who must consult with the College's Office of General Counsel prior to making or permitting any such disclosure.

f. The College as a Business Associate. At times, the College may act as a Business Associate under HIPAA. A Business Associate is a person or entity that performs certain functions or activities that involve the use or disclosure of Protected Health information on behalf of, or provides services to, a HIPAA Covered Entity. Such functions may include the arrangement, creation, reception, maintenance, or transmission of Protected Health Information for a function or activity regulated by HIPAA, data analysis, processing or administration, utilization review, quality assurance, consulting, and data aggregation. The College may be a Business Associate of a Covered Entity or of another Business Associate (i.e., a "downstream" Business Associate).

College's Administration, in consultation with the Office of General Counsel, is responsible for determining when the College is acting as a Business Associate. When the College is a Business Associate of a Covered Entity or Business Associate, the College must enter into a Business Associate agreement (a "*BAA*") that complies with the requirements of HIPAA prior to requesting or accessing any PHI provided by such entity. College's Administration, in consultation with the College's Office of General Counsel, is responsible for negotiating and signing all BAAs pursuant to which the College is a Business Associate. Each such BAA is a Data Use Agreement for the purposes of these Policies.

The Privacy Officer is responsible for understanding when the College is acting as a Business Associate and informing all applicable College Personnel. Notwithstanding the foregoing, College Personnel are expected to know and understand when their activities support the College's role as a Business Associate. In the event any College Personnel are unsure when their activities are supporting Business Associate activities, they should proactively ask the advice of their supervisor or the Privacy Officer.

When the College is a Business Associate, College Personnel will only use or disclose PHI to the extent permitted under the more stringent of: (1) any applicable requirements of HIPAA, as determined by the Office of General Counsel, and (2) the terms and conditions of the applicable BAA. In no event will any College Personnel use or disclose PHI in a manner that would violate HIPAA if the same use or disclosure were made by the applicable Covered Entity or Business Associate. Notwithstanding the foregoing, College Personnel may use or disclose PHI as necessary to comply with applicable law, including HIPAA, but only after consultation with the College's Office of General Counsel.

When the College is a Business Associate, College Personnel will not use any PHI of a Covered Entity or Business Associate to create de-identified or aggregated information unless permitted by the applicable BAA.

When the College is a Business Associate, it, in turn, must enter into "downstream" BAAs with its subcontractors before any College Personnel disclose any PHI of a Covered Entity or Business Associate to such subcontractor. College Research Administration, in consultation with the College's Office of General Counsel, is responsible for negotiating and signing all such "downstream" BAAs and ensuring their compliance with HIPAA and any applicable BAAs and other Data Use Agreements.

V. **Unauthorized Access or Disclosure**. In the event any College Personnel become aware of, or suspect, any unauthorized use, access, or disclosure of any Personal Information, such College Personnel should immediately report such actual or suspected use, access, or disclosure to the Privacy Officer who will, in turn, promptly contact the Office of General Counsel. The Office of General Counsel, together with the Privacy Officer, the CISO and any other applicable College personnel, will immediately begin a reasonable investigation and, if such unauthorized use, access, or disclosure is confirmed take reasonable steps to halt and remedy such use, access, or disclosure. College Personnel will follow the College's standard policies and procedures when responding to any actual or suspected unauthorized use, access, or disclosure.

VI. **Noncompliance with these Policies**. In the event any College Personnel become aware of, or suspect, that any College Personnel or Activity is not in compliance with these Policies, they should promptly report such actual or suspected noncompliance to the Privacy Officer. In such case, the Privacy Officer must promptly conduct a reasonable investigation and, in the event any noncompliance is found, take reasonable steps to remedy such noncompliance as soon as reasonably practicable.

VII. **Questions**. Questions about these policies should be referred to the Privacy Officer, who will consult with the CISO and Office of the General Counsel.

Audit and Accountability Policy

I. Purpose

This policy is an element of the College's Security and Privacy Policies. It sets forth the requirements for review of key auditable events to verify the appropriateness of access to Information Systems and the Data they contain, and for detection, containment and correction of security violations.

II. Scope

This policy applies to Information System Owners and IT Custodians who manage Information Systems for the College.

III. Policy

This policy defines methods that must exist in order for the College to (i) create, protect, and retain Information System logging audit records (e.g. firewall logs, system event logs, etc.) including user access audit records; (ii) regularly review, analyze and investigate unlawful, unauthorized, or otherwise inappropriate Information System activity; and (iii) ensure that the actions of individual Information System users can be uniquely traced to those users so they can be held accountable for their actions.

IV. Procedures

1. Information System Owners must maintain and document technical procedures that meet the Risk Controls set forth below when managing audit logging of Information Systems within their control.
    a. These technical procedures must account for enabling the user access audit logging functionality as well as ensuring user access audit logging reviews is occurring on a periodic basis.
    b. The documentation of these technical procedures must be retained for a period of six (6) years.
    c. In the event of a Security Incident with an Information System, then the audit logging records will be maintained by the CISO for six (6) years.

2. IT Custodians are responsible for implementing the technical procedures established by their Information System Owners for the purpose of recording and examining activity in the Information System.

3. Information System Owners are responsible for monitoring user access, and reporting anomalous activities in the Information Systems within their control to the CISO.

4. At a minimum, Information System Owners must ensure that Information Systems that store, process or transmit Restricted Information have their logging audit records (e.g. firewall logs, system event logs, etc.) including user access audit records stored as directed

by the College's IT Security team.

5. Information System Owners and IT Custodians should conform to the Data Classification Guideline when sharing audit log information. For example, an audit log with Restricted Information requires approval by the CISO, in consultation with legal counsel, when sharing with a third party.

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 as defined by the relevant impact analysis and subsequent risk analysis.

Auditable Events (AU-2 CM)	
Core	Information Systems that store, process or transmit Restricted Information must employ automated logging mechanisms that generate audit records containing adequate detail to support after-the-fact investigations of security incidents. Technical procedures for monitoring audit logs shall contain a list of the type of events considered to be being auditable. These technical procedures must provide rationale for why the type of event is considered auditable. Events to consider include: • Failed authentication attempts • Successful authentication attempts • System startup or shutdown • Use of privileged accounts (system administrator accounts) Change of user security privileges (addition of groups, password change, etc.)
Low	N/A
Moderate	The list of auditable events will be reviewed to determine its necessity and sufficiency on an annual basis and updated appropriately.
Content of Audit Records (AU-3 CM)	
Core	Audit records must contain sufficient information to establish what events occurred, when the events occurred, the source of the events, the cause of the events, and the event outcome. Elements of the audit record to consider for capture include: • Date and Time of Activity • Identification of user or process performing activity • Origin of Activity (Source and/or Destination IP address, etc.) • Description of activity (create, read, access, update)

	• Success / Failure indications • Protected Information accessed, if applicable • File accessed, if applicable Access control or flow rule invoked, if applicable
Low	N/A
Moderate	The Information System generates audit records containing additional information explicitly needed for specific audit requirements (examples: full text recording of privileged commands or the individual identities of group account users).
Audit Storage Capacity (AU-4 C)	
Core	Information Systems that store, access, or transmit Restricted Information must have a sufficient amount of system storage allocated to store the audit records in accordance to requirement AU-11. The amount of system storage can be reduced when central logging capabilities are implemented to maintain logs for the appropriate period.
Low	N/A
Moderate	N/A
Response to Audit Processing Failures (AU-5 C)	
Core	Information Systems that store, process, or transmit Restricted Information must be configured to alert the IT Custodian in the event the audit logging mechanism has failed. In the event an Information System that stores, processes or transmits Restricted Information reaches its configured capacity for audit log retention, the Information System must be configured to overwrite the oldest audit logs If possible, and not detrimental to business functions, the system can be configured to halt its processing until the audit capturing functionality is restored.
Low	N/A
Moderate	N/A
Audit Monitoring, Analysis, and Reporting (AU-6 CM)	
Core	Suspicious, unusual or malicious activity must be reported to the College's IT Security team.
Low	Reviews of audit records must occur at least on a routine basis for Information Systems that store, process, or transmit Restricted Information.
Moderate	Audit logs will be reviewed, analyzed and reported in an automated manner leveraging the College's centralized log management system.

Audit Reduction and Report Generation (AU-7 CM)	
Core	The central log management system operated by the College's IT Security team shall provide a means to generate reports for audit review, analysis, and after- the-fact investigations of security incidents. The reduction of audit content (i.e. audit information provided in a summary format) will not alter the original audit content or time ordering of audit records.
Low	N/A
Moderate	The central log management system operated by the College IT Security team will automatically process audit records and generate reports for events of interest based on, at a minimum, user, process, or network address.
Time Stamps (AU-8 C)	
Core	Information System audit logs must employ time stamps. Time stamps of audit records must be generated using internal system clocks that are synchronized system-wide either to the UCM time management server, the BSD time management server, or the College time management server. Time stamps will record time based on the Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). If practicable, the time stamp will also record the local time offset from UTC (-6 hours)
Low	N/A
Moderate	N/A
Protection of Audit Information (AU-9 CM)	
Core	The Information System will be configured to protect audit information with the minimum necessary access, to prevent unauthorized access, modification and deletion.
Low	N/A
Moderate	Only IT Custodians of the Information System or the College IT Security team may access the audit functionality of the Information System.
Audit Record Retention (AU-11 C)	
Core	Information Systems that store, process or transmit Restricted Information must maintain user access audit logs for a minimum of three (3) months.
Low	N/A
Moderate	N/A
Audit Generation (AU-12 LM)	

Core	Information Systems that store, process or transmit Protected Information must: • Provide audit record generation capabilities that meets AU-2 Information Systems must either a) send audit log data to the central log management system operated by the College IT Security team in real time, or b) produce audit log content within 1 hour of the request to the College IT Security team.
Low	N/A
Moderate	N/A

VI. Interpretation, Implementation and Revision

The CISO, with the support of IT Custodians and the Office of General Counsel, is responsible for the interpretation and implementation of this policy and recommending revisions of this policy to the College.

Access Control Policy

I. Purpose

This policy is an element of the College's Security and Privacy Policies. It sets forth a general framework for user account management, access enforcement and monitoring, separation of duties, and remote access for systems 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 College's Information. All Covered Individuals are subject to this policy.

III. Policy

The CISO will define access rules that will ensure that all Covered Individuals who are entitled to access Information Systems and Information, including Protected Information, can do so, and will ensure that those who are not entitled to access Information Systems and Information, including Protected Information, cannot do so. Access rights are determined based upon the Security Obligations. The CISO is responsible for defining the process and procedures for authorizing, establishing, documenting, reviewing, and modifying access to Information Systems and Information. Access is subject to privacy laws and policies as well as contractual obligations.

IV. Procedures

1. Each Information System Owner is responsible for identifying the IT Custodians for each Information System under their control.
2. Each Information Owner will identify the individuals, groups of individuals and/or roles of individuals, who may access the Information System and the Information under his/her control, and for each, the appropriate access level.
3. Each Information System Owner will establish and document the user account management, access monitoring, and remote access technical procedures that apply to the each Information System he/she controls.
4. Each IT Custodian will ensure that the technical procedures meet the Risk Controls set forth below when managing (including granting and revoking) access the Information Systems and the Information stored on the Information System within their control.
5. The Information System Owner will document the identification of all of the individuals, groups, and roles with access rights, along with their respective permitted access levels; all access management activity will be documented. This documentation will be retained for a six (6) years after termination of the access grant.
6. The Information System Owner, in collaboration with the Information Owner, will routinely check that User access is appropriate.
7. Information System Owners must ensure that access for Covered Individuals who no longer require access to Information and Information Systems will have their access promptly removed in accordance with the College's human resources and contractor policies and procedures. E.g. an employee has left the College, or an employee has

changed job responsibilities.

8. The CISO, in consultation with legal counsel and human resources departments, determines the situations in which access to an Information System under the CISO's authority may be terminated with or without prior notice to the user, as appropriate under the circumstances.

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.

Access Control Procedures (AC-1 C)	
Core	The CISO defines access rules 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.
Low	N/A
Moderate	N/A
User ID and Account Management (AC-2 CLM)	
Core	Comprehensive technical account management procedures must be established to: identify account types (i.e., individual, group, and system); establish conditions for group membership; and assign associated authorizations. User ID must uniquely identify only one user. Shared or group user IDs must not be created or used on Information Systems with Protected Information, unless approved by the College's Information Security Office. User IDs for inactive accounts must be periodically disabled. Account control mechanisms shall be in place and supporting procedures are developed, documented and implemented effectively to authorize and monitor the use of accounts; and to remove, disable, or otherwise secure unnecessary accounts.
Low	Accounts must be re-evaluated periodically to determine whether account access is needed to perform the user's current job duties.
Moderate	The information System must automatically: • Remove or disable temporary and emergency accounts after 180 days. • Disable inactive accounts after 180 days.

	• Audit account creation, modification, enabling, disabling, and removal actions, and notifies Information System Owners.
Access Enforcement and Restrictions (AC-3 CL)	
Core	Users must be positively identified (e.g. basic authentication, challenge/response, time-based code sequences, or PKI) prior to being able to use any multi-user computer or information system resource. When passwords are used, the standards identified in the IT Services operating procedures must be followed. Access enforcement rules must be documented by the Information System Owner.
Low	For users with similar duties, groups or role-based access controls (RBAC) must be used to assign access to individual accounts based on job descriptions, duties or function and the authorizations (or privileges) to perform the needed operations.
Moderate	N/A
Information Flow Enforcement (AC-4 M)	
Core	N/A
Low	N/A
Moderate	Information Systems must be configured to restrict network based and logical based access, and restrict the transfer of Restricted Information to Information Systems not designated to house Restricted Information. This can be accomplished by: • Prohibiting Information transfers between interconnected Information Systems. • Employing hardware mechanisms to enforce one-way Information flows. • Implementing regarding mechanisms to re-assign security controls to downstream Information Systems.
Separation of Duties (AC-5 M)	
Core	N/A
Low	N/A
Moderate	Access control software shall be in place to limit individual authority and information access that ensure that no one individual has exclusive control over the process (e.g. IT Custodians administering access control functions do not also administer audit functions). Job descriptions shall reflect accurately the assigned duties and responsibilities that support separation of duties. Information System owners must develop procedures that:

	• Separate organization-defined duties of individuals. • Document separation of duties of individuals. • Define Information System access authorizations to support separation of duties.
Least Privilege (AC-6 CM)	
Core	Users are only granted privileges necessary to accomplish their assigned task in accordance with mission and business functions. Access to privileged accounts (accounts that administer the Information System) must be restricted to specific IT Custodians or roles. IT Custodians or Covered Individuals with privileged accounts must use only the privileged account for administrative purposes; IT Custodians or Covered Individuals will use regular, non-privileged accounts, for general access needs.
Low	N/A
Moderate	Each user or process shall be assigned the most restrictive set of privileges needed for the performance of authorized tasks. The Information System must audit the execution of privileged functions and prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.
Unsuccessful Login Attempts (AC-7 CM)	
Core	The information System must enforce a limit of consecutive invalid logons and either automatically lock the account or delay the next logon prompt when the maximum number of invalid logons is reached.
Low	N/A
Moderate	N/A
System Use Notification (AC-8 LM)	
Core	Information Systems shall display to users a notification message or banner before granting access that provides privacy and security notices and states that: • Users are accessing the College's Information System. • Information system usage may be monitored, recorded, and subject to audit. • Users who logon represent that they are authorized to do so. • Unauthorized use of the information system is prohibited and subject to criminal and civil penalties. • Use of the information system indicates consent to monitoring and

	recording.
Low	N/A
Moderate	Information Systems must retain the notification message or banner on the screen until users acknowledge the usage conditions. Publicly accessible Information Systems should include a description of the authorized uses of the system.
Session Lock (AC-11 M)	
Core	Endpoints will be configured to automatically lock after 15 minutes of inactivity, unless the Endpoint is a dedicated-function device used in research, instruction, health care, telephony, building automation systems, or other activities.
Low	N/A
Moderate	Information Systems shall prevent access to the system by initiating a session lock after a defined time period of inactivity or upon receiving a request from a user; and retain the session lock until the user reestablishes access using proper authentication procedures. The Information System conceals information previously visible on the screen during its lockout.
Session Termination (AC-12 M)	
Core	N/A
Low	N/A
Moderate	Information Systems automatically terminate a User's session after a period of 8 hours. The Information Systems shall provide a logout capability for user sessions whenever authentication is used to gain access to information assets, and an explicit logout message shall be displayed to users indicating the reliable termination of authenticated sessions.
Permitted Actions w/o Identification or Authentication (AC-14 LM)	
Core	N/A
Low	Information Systems will be configured to permit public access, without User identification and authentication, only to the extent necessary to accomplish mission objectives. Information System Owners will document the rational for not requiring identification or authentication.
Moderate	N/A
Remote Access (AC-17 CLM)	
Core	All remote access connections must be through a secure, centrally administered point of entry approved by the CISO (e.g. cVPN).

	Remote access to Information Assets is provided solely for the purpose of accomplishment of the College's mission and objectives. Any other use is strictly prohibited. Cryptographic mechanisms, approved by the CISO, must be used to protect the confidentiality and integrity of remote access sessions.
Low	Personally owned computer equipment used for remote access must be approved and must also comply with the cyber security policies and procedures and standards. All remote access connections must be monitored for the detection of cyber- attacks.
Moderate	The authority to executive privileged commands and access security plans via remote access is limited to Information System Owners that have a need for such access. The rational for such access is documented into the system's security plan.
Wireless Access (AC-18 LM)	
Core	Secure wireless networks will require the use of authentication and encryption prior to providing access to the College or UCMC network. Use of the College's wireless networks will only be permitted when leveraging the secure wireless capabilities provided by the College. Covered Individuals will only use secure wireless networks, and will not use unsecure networks (e.g. guest networks) without first initiating a VPN connection for the College's related use.
Low	N/A
Moderate	N/A
Access Control for Portable and Mobile Devices (AC-19 CLM)	
Core	The storage and transmission of Restricted Information on portable and mobile devices shall be protected with activities such as scanning the devices for malicious code, virus protection software, and disabling unnecessary hardware, regardless of device ownership. Mobile devices that store or transmit Restricted Information must all criteria in the College's Baseline Expectations for End User Devices policy.
Low	N/A
Moderate	Mobile devices must be specifically authorized to connect to Information Systems.
Use of External Information Systems (AC-20 C)	
Core	Before any third-party partner is given access to an Information System, a contract defining the terms and conditions of said access must be in place that has been reviewed and approved by legal counsel.

Low	N/A
Moderate	N/A
Information Sharing (AC-21 CM)	
Core	N/A
Low	N/A
Moderate	Sharing of Restricted Information outside of the College occurs only in partnership and compliance with the policies of College Research Administration, Office of General Counsel, Institutional Review Boards, Office of Corporate Compliance, or other applicable College policies.
Publicly Accessible Content (AC-22 CM)	
Core	Users must not place Restricted Information on any publicly accessible Information System unless the posting has been approved by Office of General Counsel. Information destined to be posted on publically accessible Information Systems must be reviewed for nonpublic Information and authorized to be posted by the cognizant Department or Unit leader.
Low	N/A
Moderate	Covered Individuals, authorized by Department or Unit leaders, shall review content on publicly accessible Information Systems for nonpublic information on an organization-defined frequency and notify the CISO if discovered.

VI. Interpretation, Implementation and Revision

The CISO, with the support of IT Custodians and the Office of General Counsel, is responsible for the interpretation and implementation of this policy and recommending revisions of this policy to the College.

Configuration Management Policy

I. Purpose

This policy is an element of the College's Security and Privacy Policies. It ensures the College's Information Assets are managed in a secure manner, and that the information stored, transmitted or processed are protected and secure.

II. Scope

This policy applies to Information Assets (workstations, laptops, mobile devices, servers, software applications, enterprise applications, etc.) that are owned by the College. All Covered Individuals are subject to this policy. Information Assets not owned by the College (e.g. personally owned devices, third parties) are subject to different requirements.

III. Policy

The CISO will define Standards to (i) establish and maintain security baseline configurations (ii) ensure inventories of the College's Information Assets (including hardware, software, firmware, and documentation) are managed and maintained throughout the respective Information Asset life cycles, and (iii) process to manage changes to the Information Assets.

IV. Procedures

1. Information System Owners must maintain and document technical procedures that meet the Risk Based Controls set forth below and comply with Standards. IT Custodians must implement the documented technical procedures that meet the Risk Based Controls set forth below. Information System Owners and IT Custodians may seek guidance from the University CISO in developing technical procedures.

2. Information System Owners are responsible for maintaining an inventory of Endpoints and Information Systems managed within their purview. The inventory must be produced by the Information System Owner to the CISO upon reasonable request. At a minimum, the inventory must include the following information:
    a. Hostname
    b. MAC address (wired)
    c. MAC address (wireless)
    d. Primary User (or appropriate designation if the asset is shared)
    e. Owning Department/Unit
    f. Device Type (server, workstation, laptop, mobile device)
3. Covered Individuals who manage their own Endpoints and Information Systems without support from an IT services group must register and maintain their Endpoints and Information Systems in accordance with standards and procedures as may be required by the CISO.
4. Information System Owners are responsible for ensuring changes to their Information

Systems have been documented and reviewed through a change control process. The change control process must be approved by the CISO.

5. It is the responsibilities of the Information System Owners to retain all the documents referenced above.

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 as defined by the impact analysis and subsequent risk analysis.

Baseline Configuration (CM-2 CM)	
Core	Technical procedures must be developed, documented and maintained which define the baseline configurations for their Information Assets (endpoints, servers, etc). These baselines will be managed leveraging versioning and configuration control.
Low	N/A
Moderate	Review and update the baseline configurations of Endpoints and Information Systems on a periodic basis and as an integral part of Information System component installations and upgrades. Retain at least one (1) previous version of baseline configurations to support rollbacks, if necessary. As may be required by the CISO, Endpoints with a higher baseline security standard to Covered Individuals will be used when traveling to countries of significant risk and apply additional sanitization safeguards to those Endpoints when the Covered Individuals return.
Configuration Change Control (CM-3 CM)	
Core	Changes to baseline configurations of Endpoints and Information Systems will be managed in accordance with applicable change management procedures.
Low	N/A
Moderate	Changes must be tested, validated and documented before making the change to any Information Asset. The procedures should include, at a minimum: a. The change request process with related forms and work flow b. Test plan requirements c. Emergency change procedures Change requests must be reviewed and approved by the appropriate Information System Owner, or other Departmental or Unit Leader, prior to the change being authorized.

	Emergency changes to an Information Asset must be documented and approved by an Emergency Change Advisory Board. All emergency changes must be reviewed post change by the CAB. Documentation of change control must be kept for a period of six (6) years by the applicable IT Custodian
Security Impact Analysis (CM-4 CL)	
Core	Changes to Information Assets will be analyzed to determine potential security impacts prior to change implementation. This analysis can occur through the normal and regular CAB meetings.
Low	Authorized security personnel conduct security impact analyses, which should include, but is not limited to, risk analysis, reviewing security plans to understand security control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls.
Moderate	N/A
Access Restrictions for Change (CM-5 M)	
Core	N/A
Low	N/A
Moderate	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the Information System, including at a minimum: • Limit to specific roles the privilege to change Information System components and system-related information within a production or operational environment Limit privileges to change software resident within software libraries Review and reevaluate change privileges on a periodic basis
Configuration Settings (CM-6 CL)	
Core	Configuration settings must be established, documented and implemented that are specific to the Information Asset that reflect the most restrictive operational mode possible while maintaining operational requirements.
Low	Deviations from baseline configuration settings must be approved by the CISO. Changes to configuration settings must be submitted, and approved, through the change control procedures.
Moderate	N/A
Least Functionality (CM-7 CM)	

Core	Information Assets must be configured to provide only essential capabilities. The functions and services provided by Information Assets must be reviewed carefully to determine which functions and services are candidates for elimination or restriction (e.g., File Transfer Protocol [FTP], Hyper Text Transfer Protocol [HTTP] etc.). The use of those non-essential functions, ports, protocols, and/or services must be prohibited and/or restricted.
Low	N/A
Moderate	Information Assets shall be reviewed on a periodic basis to identify unnecessary and/or non-secure functions, ports, protocols, and services. Functions, ports, protocols, and services within the Information Asset deemed to be unnecessary and/or non-secure shall be disabled. Approved software programs will be managed and inventoried and Information Assets will be configured to prevent execution of unauthorized software. This shall be done through an allow-all or deny-by-exception policy. Approved software programs will be reviewed and updated on a periodic basis.
Information System Component Inventory (CM-8 LM)	
Core	Procedures must be developed to document and maintain a current inventory of Information Assets and relevant ownership information, as defined within the Procedures section of this policy. Inventory shall be reviewed and updated as need/required.
Low	N/A
Moderate	Inventory lists will be managed as part of regular Information Asset maintenance. Management of Information Assets will be conducted through automated mechanisms which will, at a minimum: a. Detect presence of unauthorized software, hardware and firmware components b. Update Information Asset ownership information to be current c. Automatically enforce restrictions on the Information Asset if unauthorized components are detected Information Asset components will be verified within its authorization boundary of the Information System to ensure it is not duplicated in other Information System component inventories.
Configuration	

Management Plan (CM-9 M)	
Core	N/A
Low	N/A
Moderate	A Configuration Management Plan must be developed, documented and maintained that: a. Addresses the roles, responsibilities, and configuration management processes and procedures. b. Establishes a process for identifying configuration items throughout the system development life cycle (SDLC) and management of the configuration of the configuration items. c. Defines the configuration items for the Information Assets and place the configuration items under configuration management. Protects the configuration management plan from unauthorized disclosure and modification.

Software Use Restrictions (CM-10 CL)	
Core	Procedures must be developed, documented, and implemented effectively to limit the use of software for only licensed purposes and according to contract agreements and copyright laws.
Low	Software licenses, and associated documentation, will be tracked by quantity of licenses to control the copying and distribution. Use of peer-to-peer file sharing technologies will be controlled to ensure this capability is not used for unauthorized distribution, display, performance or reproduction of copyrighted work.
Moderate	N/A

User Installed Software (CM-11 L)	
Core	N/A
Low	Information Assets will be configured in a manner that: a. Prohibits the installation of software by users b. Enforces software installation through central management methods Is monitored for compliance with these restrictions on a periodic basis
Moderate	N/A

VI. Interpretation, Implementation and Revision

The CISO, with the support of IT Custodians and the Office of General Counsel, is responsible for the interpretation and implementation of this policy and recommending revisions of this policy to the College.

Physical and Environmental Protection Policy

I. Purpose

This policy is an element of the College's Security and Privacy Policies. It defines requirements for the physical, environmental controls and facility access controls to ensure the protection of Information Assets and Information Systems from unauthorized access and safeguard against environmental threats.

II. Scope

This policy applies to Designated Secure Computing Facilities (e.g. data centers, server rooms, data closets, etc.) and some parts apply to Information Assets (e.g. workstations) within public areas accessible to non-Covered Individuals (e.g. waiting area, lobby, train etc.). All Covered Individuals are subject to this policy.

III. Policy

This policy defines the physical and environmental controls that must exist to protect Information Assets and Information Systems from unauthorized access and safeguard against environmental threats. The College requires that (i) its facility and equipment are safeguarded from unauthorized physical access, tampering and theft by only allowing access to those who are entitled to have physical access to Information Assets and Information Systems; (ii) preventing access by those who are not entitled to access Information Assets and Information Systems; and (iii) protecting the environment through proper management and maintenance to allow for the reliable operation of the Information Assets and Information Systems.

IV. Procedures

1. Information System Owners must ensure that their Information Systems are housed in a Designated Secure Computing Facility (DSCF) that meets the requirements of this policy.

2. Each Department and Unit Leader who oversees a DSCF, or rooms containing network equipment, wiring, or telecommunications, will:

    a. Develop technical procedures that meet the Risk Based Controls set forth below when managing the security and environmental controls (e.g. HVAC, emergency power shut off, fire suppressant, humidity control, cabling, etc.).

    b. Develop procedures for the authorization of, and keep a record of the authorization of, all Covered Individuals with a need to access the DSCF.

    c. Develop procedures for the revocation of access.

    d. Ensure that Information Systems or Information Assets housed in a DSCF are physically secured in a manner that provides access to only those Covered Individuals they authorize.

    e. Ensure that all Covered Individuals within the DSCF are wearing the appropriate badge that distinguishes them from a visitor. All visitors will be identified as such with the appropriate badge. Temporary badges that provide access to the DSCF must expire after a set period of time.

f. Review the physical security and environmental controls of the DSCF on a periodic basis and consult with the CISO to ensure continued adherence to this policy.

g. Document repairs and modifications to the physical components of the facility which are related to security (e.g. hardware, doors, walls and locks).

3. Each IT Custodian is responsible for ensuring that Information Assets in public areas have appropriate physical safeguards in place to prevent theft of the Information Assets.

4. Each IT Custodian is responsible for ensuring that Information Assets in public areas used to process, store or transmit Restricted Information are set up in a manner that prohibits the incidental viewing of the display screen.

IV. 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.

Physical and Environmental Protection Policy and Procedures (PE-1 C)	
Core	The CISO will define the proper physical and environmental controls, pursuant to this policy, which must be implemented by Information System Owners and IT Custodians.
Low	N/A
Moderate	N/A
Physical Access Authorizations (PE-2 CM)	
Core	Each DSCF, network, wiring or telecommunications room, must have access limited to authorized individuals. Access to the DSCF, network, wiring or telecommunications room, will be granted through a physical security system. Access to the DSCF, network, wiring or telecommunications room, will be revoked once it is no longer needed. Authorized access to the DSCF, network, wiring or telecommunications room, will be reviewed at least annually.
Low	N/A
Moderate	Visitor access to a DSCF will either require two forms of identification that positively identifies the visitor prior to granting access, or be permitted only under escort by an authorized Covered Individual.
Physical Access Control (PE-3 C)	
Core	Access to a DCSF must be protected through the use of a technology that limits access only to bearers of individually authorized access tokens, e.g., an ID card reader.

	Access to a network, wiring or telecommunications room should be protected through the use of a technology that limits access only to bearers of individually authorized access tokens, but may be protected by key or combination access if permitted by the CISO. Physical access audit logs to a DSCF, network, wiring or telecommunications room, will be maintained and recorded for all Covered Individuals, including visitors, and retained for at least 90 days. Visitors to a DSCF, network, wiring, or telecommunications room, are escorted and visitor activity is monitored in all circumstances. Keys, combinations, and other physical access devices to a DSCF, network, wiring or telecommunications room, must be secured and inventoried. Keys, combinations, and other physical access devices to a DSCF, network, wiring or telecommunications room, are changed when keys are lost, combinations are compromised, or a Covered Individual with access to a combination is terminated or job duties change.
Low	N/A
Moderate	N/A
Access Control for Transmission Medium (PE-4 M)	
Core	N/A
Low	N/A
Moderate	Locked wiring closets and disconnected spare jack safeguards must be in place to control physical access to system distribution and transmission lines.
Access Control for Output Devices (PE-5 M)	
Core	N/A
Low	N/A
Moderate	Information Assets with output devices (displays, monitors, printers, copiers, scanners, etc.) must be deployed in a manner that prevents unauthorized individuals from obtaining the output.
Monitoring Physical Access (PE-6 CL)	
Core	Access to a DSCF: a. Must be monitored to detect physical security incidents through the use of intrusion alarms (e.g. door open alarms, tampering alarms, etc.) or video surveillance equipment.

	b. Physical access logs are reviewed periodically and for occurrence of any intrusion alarms. Security incidents to the DSCF, wiring and telecommunication rooms must be reported to campus safety and the IT Security Office.
Low	When video surveillance is used for monitoring, recordings must be kept for a period of ninety (90) days.
Moderate	N/A
Visitor Access Records (PE-8 LM)	
Core	Visitor Access Records: a. Must be maintained for a period of one (1) year. Must be reviewed on a periodic basis.
Low	N/A
Moderate	N/A
Power Equipment and Power Cabling (PE-9 M)	
Core	N/A
Low	N/A
Moderate	Power equipment and power cabling within a DSCF, network, wiring or telecommunications room, must be protected from damage and destruction.
Emergency Shutoff (PE-10 M)	
Core	N/A
Low	N/A
Moderate	The DSCF: a. Must contain a mechanism for shutting off power to Information Systems in emergency situations. b. Must have emergency shutoff switches or devices in locations that facilitate safe and easy access for personnel. Emergency power shutoff must be protected from unauthorized and accidental activation.
Emergency Power (PE-11 M)	
Core	N/A
Low	N/A
Moderate	The DSCF must contain short-term uninterruptible power supply to facilitate either an orderly shutdown of Information Systems or transition of Information Systems to long-term alternate power in the event of a primary

	power source loss.
Emergency Lighting (PE-12 L)	
Core	N/A
Low	The DSCF employs and maintain automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes.
Moderate	N/A
Fire Protection (PE-13 CM)	
Core	The DSCF must contain, employ and maintain fire suppression and detection devices/systems that are supported by an independent energy source.
Low	N/A
Moderate	The DSCF employs an automatic fire suppression capability when it is not staffed on a continuous basis.
Temperature and Humidity Controls (PE-14 C)	
Core	The DSCF must contain an environmental management system that continuously monitors and maintains temperature and humidity levels within the facility where Information Systems resides at a level consistent with ASHRAE Thermal Guidelines for Data Processing Environments.
Low	N/A
Moderate	N/A
Water Damage Protection (PE-15 C)	
Core	The DSCF will employ safeguards that protect from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.
Low	N/A
Moderate	N/A
Delivery and Removal (PE-16 LM)	
Core	All movement of Information Systems and Information System components into and out of the DSCF, network, wiring or telecommunications rooms are authorized, monitored, and controlled.
Low	Records of the movement of Information Systems and Information System components into and out of the DSCF, network, wiring or telecommunications rooms are maintained.
Moderate	N/A

Alternate Work Site (PE-17 M)	
Core	N/A
Low	N/A
Moderate	Procedures must be developed, documented, and implemented effectively to control security at alternate work sites which aligns with the College's business continuity and contingency plans.

VI. Interpretation, Implementation and Revision

The CISO, with the support of IT Custodians and the Office of General Counsel, is responsible for the interpretation and implementation of this policy and recommending revisions of this policy to the College.

Electronic Media Protection Policy

I. Purpose

This policy is an element of the College's Security and Privacy Policies. It sets forth the procedures for safeguarding the Electronic Media that store Restricted Information to ensure that privacy, security, and integrity of Restricted Information is maintained and to guard against the improper disclosure and access to unauthorized individuals consistent with the Security Obligations.

II. Scope

This policy applies to Electronic Media that stores the College's Restricted Information. All Covered Individuals are subject to this policy.

The term "**Electronic Media**" means electronic storage devices on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card.

III. Policy

The College's Chief Information Security Officer, in consultation with the Office of Legal Counsel, determines the standards under which all Information, including Restricted Information, can be stored, and sets the standards and/or requirements applicable to the procurement, deployment, use and disposal of Electronic Media.

IV. Procedures

1. Covered Individuals will use Electronic Media devices that are approved by the CISO when using, accessing, storing, and moving Restricted Information. The CISO ensures these Information Security Standards are available to all Covered Individuals.

2. The CISO establishes controls and procedures applicable to generally available Electronic Media (e.g. thumb drives, external hard drives, hard drives, etc.) while each Information System Owner establishes controls and procedures applicable to the Information Systems under their control. Departmental and Unit Leaders insure that Covered Individuals under their supervision abide by the policies and procedures created by the CISO and Information System Owners.

3. Electronic Media that contains Restricted Information will be secured in the manner set by the CISO (e.g. encryption, etc.) when physically moving the Restricted Information (both within and outside of the College). The CISO will ensure these Information Security Standards are available to all Covered Individuals.

4. Information System Owners, or IT Custodians, implement procedures that apply to the movement of hardware and Electronic Media.

5. The CISO establishes procedures for the disposal or re-use of Electronic Media to ensure that Restricted Information is removed from the Electronic Media before it is disposed of or made available for re-use.

6. Any agreement in which the College's Restricted Information is shared with a third party will require return or destruction of the College's Restricted Information, unless exception is granted by Office of Legal Counsel. At the direction of the Privacy Officer or CISO, a third party will certify that it returned or destroyed the Restricted Information.

7. The CISO will include in the content for Security Training the appropriate way in which to sanitize and/or dispose of Electronic Media that contains Restricted Information. The CISO will ensure these Information Security Standards are available to all Covered Individuals.

8. Covered Individuals can use unencrypted Electronic Media devices for the storage of Internal or Public Information as defined in the College's Data Classification Guideline.

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.

Media Protection Policy and Procedures (MP-1 C)	
Core	The CISO establishes controls and procedures applicable to generally available Electronic Media (e.g. thumb drives, external hard drives, hard drives, etc.) while each Information System Owner establishes controls and procedures applicable to the Information Systems under their control, and Departmental and Unit Leaders insure that Covered Individuals under their supervision abide by the policies and procedures created by the CISO and Information System Owners.
Low	N/A
Moderate	N/A
Media Access (MP-2 CL)	
Core	Electronic Media will have access restricted to the appropriate personnel or role- holders with a business need.
Low	Procedures will ensure access to physical Electronic Media inside of Information Systems is restricted.
Moderate	N/A
Media Labeling (MP-3 CM)	

Core	If Restricted Information stored on Electronic Media is intended to be transferred out of its Designated Secure Computing Facility, the physical Electronic Media must be labeled in a manner whereby it can be traced back to the department or unit that owns the Electronic Media.
Low	N/A
Moderate	Physical Information Systems in which Restricted Information is stored, or any physical Electronic Media removed from such an Information System, shall have external labels affixed to indicate the distribution limitations, applicable security classification, and handling caveats of the Restricted Information.
Media Storage and Inventory (MP-4 CL)	
Core	Endpoints and Electronic Media used for the storage of Restricted Information must be encrypted. Electronic Media must be controlled physically and safeguarded in the manner prescribed for Restricted Information until the media are destroyed or sanitized in accordance with this policy. Inventory and disposition records for Information System Electronic Media must be maintained to ensure control and accountability of the Information.
Low	Media inventory records must contain sufficient data to effectively identify the owner, content and age of the media.
Moderate	N/A
Media Transport (MP-5 C)	
Core	N/A
Low	N/A
Moderate	Electronic Media must be encrypted with a FIPS 140-2 validated encryption algorithm, or stronger, when physically transported outside of a Designated Secure Computing Facility.
Media Sanitization and Disposal (MP-6 CM)	
Core	All Electronic Media with Protected Health Information or Personally Identifiable Information must be sanitized prior to disposal, release out of organizational control, or released for reuse. Disposal and sanitization procedures must be approved by the CISO.
Low	N/A
Moderate	All Electronic Media with Restricted Information must be sanitized prior to disposal, release out of organizational control, or released for reuse, consistent Security Obligations. Sanitization equipment and procedures are tested at least annually to ensure proper functionality.

Media Use (MP-7 LM)	
Core	N/A
Low	The use of mobile Electronic Media in Information Systems that store, process, or transmit Restricted Information is restricted when such Electronic Media have no identifiable owner.
Moderate	N/A

VI. Interpretation, Implementation and Revision

The CISO, with the support of IT Custodians and the Office of General Counsel, is responsible for the interpretation and implementation of this policy and recommending revisions of this policy to the College.

Personally Owned Device Policy

I. Purpose

This policy is an element of the College's Security and Privacy Policies. It sets the baseline expectations for the use of personal devices by Covered Individuals in connection with the College's Information.

II. Scope

This policy applies to personally owned devices used to store, process or transmit the College's Information. All Covered Individuals are subject to this policy.

Dedicated Function devices, e.g., biomedical devices, lab instruments or building management devices, are not in scope for this policy.

III. Policy

The CISO, in consultation with the Office of Legal Counsel, determines the standards under which a Covered Individual's personally owned Information Assets can be used for the processing, storing or transmitting of the College's Information.

Covered Individuals are permitted to use a personally owned device (e.g. smartphone, tablet, laptop, desktop) for accessing the College's Information or Information Systems. Covered Individuals, if electing to use their personally owned Information Asset for the College's intended purposes, will permit Information System Owners and IT Custodians to implement security controls upon their personally owned devices, as outlined below, or will respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings.

All cyber security policies apply to all devices that access the College's Information Systems regardless of whether the device is owned by the College, owned by the User, or owned by a third party.

IV. Procedures

1. The CISO is responsible for educating Covered Individuals on (a) the capabilities of commonly used personally owned devices that store Restricted Information, and (b) the College's rights to enforce security restrictions set forth in (3) and (4) below.

2. Covered Individuals who access or store Restricted Information on their personally owned devices will follow the privacy and cyber security policies and procedures that apply to the Restricted Information they are accessing and storing; examples include encrypting the device before downloading Restricted Information, using a username and password/passcode as defined in the Access Control Policy to secure the device, and using antivirus software on laptops and desktops.

3. The CISO has the right to enforce (through procedures and/or technology) device encryption of a Covered Individual's personally owned device when that Covered

Individual uses that personally owned device to access the College's Information.

4. The CISO has the right to enforce (through procedures and/or technology) the rule that the personally owned device is automatically erased if a Covered Individual enters more than ten (10) incorrect passwords or passcodes to unlock the device.

5. Devices not administered under the authority of the College or its Covered Individuals may not be used to access or store the College's Information Systems or Restricted Information (e.g. hotel computers).

6. Covered Individuals must:
   a. Destroy, remove and upon request return all Information of the College from their personally owned device when their relationship with the College ends or when they are no longer the owner or primary user of the personally owned device.
   b. Remove or return all software applications licensed by the College when the software application or the personally owned device is no longer used for the College's business purposes.
   c. Not provide access to the College's Information to any third party, either by sharing the personally owned device or showing the personally owned device to a third party.
7. Covered Individuals must understand and agree:
   a. At no time does the College accept responsibility for the maintenance, backup, or loss of Information on a personally owned device. It is the responsibility of the Covered Individual to ensure any backups are encrypted.
   b. The College shall not be responsible for the loss, theft, or damage of a personally owned device. This includes, but is not limited to, a device used by its owner in the College's business, on the College's time, or during business travel sanctioned by the College.
   c. The College at no time accepts responsibility for the security of the personally owned device. The security of the device is the responsibility of the Covered Individual.

V. Interpretation, Implementation and Revision

The CISO, with the support of IT Custodians and the Office of General Counsel, is responsible for the interpretation and implementation of this policy and recommending revisions of this policy to the College.

Awareness and Training Policy

I. Purpose

This policy is an element of the College's Security and Privacy Policies. The College trains Covered Individuals on the policies and procedures regarding the security of Restricted Information, Information Assets and 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

This policy applies to the Covered Individuals who use, store, process and transmit the College's Information.

III. Policy

The Privacy Officer, in consultation with the Office of General Counsel, will determine whether non-employed individuals are members of the College's Covered Individuals.

The CISO and the Privacy Officer, in consultation with the Office of General Counsel, determines the content, scope, and delivery mechanism of awareness campaigns and training regarding information security consistent with each College's Security Obligations ("**Security Training**"). Covered Individuals are required to participate in Security Training that is relevant to their work.

IV. Procedures

1. Training and Awareness Leadership

The College delegates to the CISO the responsibility for Security Training content and working with departments to ensure Security Training content is included in the College's Security Training activities and programs. The CISO will ensure that the Security Training content complies with the other policies of the College. In addition, the CISO will ensure that the College's Security Training content and programs are consistent and not conflicting. Security Training content for Information System Owners and other Covered Individuals will include: guarding against, detecting and reporting malicious software, monitoring log-in attempts and reporting discrepancies, and creating, changing, and safeguarding passwords.

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

The CISO will provide and/or facilitate, and each Covered Individual will participate in, Security Training related to Restricted Information on at least an annual basis. At the discretion of the CISO, the Privacy Officer, or College Office of Legal Counsel, the CISO will provide and/or facilitate additional Security Training to Covered Individuals (a) in response to an incident, (b) based upon the individual's role or function, (c) based upon the nature of the Restricted Information, and/or (d) as needed to ensure the College adheres to the Security Obligations. The 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 College will actively participate in the Security Training as directed by their supervisor or other leader.

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

The CISO will provide and/or facilitate Security Training, and each Covered Individual will participate in, related to Restricted Information when they join their College. 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 College will actively participate in the Security Training as directed by their supervisor or other leader.

4. Documentation

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

The College 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 College delegates to the CISO the responsibility for Security Training content and working with departments to ensure Security Training content is included in the College's Security Training activities and programs. The CISO will ensure that the Security Training content complies with the other policies of the College. In addition, the CISO will ensure that the College's Security Training content and programs are consistent and not conflicting. Supporting procedures shall facilitate the implementation of this policy. The supporting procedures are subject to annual review and update.
Low	N/A
Moderate	N/A
Security Awareness Training (AT-2 CM)	
Core	Security Training is included for new users to the College as part of the new employee/contractor's orientation program.

Low	N/A
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)	
Core	N/A
Low	Certain Covered Individuals receive Security Training specific to their business function on an annual basis. IT Custodians receive appropriate Security Training as it relates to the security management and operations of their Information Systems.
Moderate	N/A
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.
Low	N/A
Moderate	N/A

VI. Interpretation, Implementation and Revision

The CISO, with the support of IT Custodians and the Office of General Counsel, is responsible for the interpretation and implementation of this policy and recommending revisions of this policy to the College.

System and Information Integrity Policy

I. Purpose

This policy is an element of the College's Security and Privacy Policies. It ensures Information System flaws are identified, reported and corrected in a timely manner, provides protection from malicious code and ensures Information System's security alerts are monitored and actions are taken in response to said alerts.

II. Scope

This policy applies to all Information Systems used to store, process and transmit the College's information. All Covered Individuals are subject to this policy.

III. Policy

The College's CISO determines the security standards under which all Information Systems will operate. Security controls implemented are based upon the Security Obligations and will focus on (i) the management in Information System flaws, (ii) minimizing the impacts of malicious code, and (iii) ensuring that security alerts generated by Information Systems are managed and responded to in an appropriate manner.

This policy supports the College's goals of (i) corroborating that Restricted Information has not been altered, modified or destroyed in an unauthorized manner, (ii) guarding against unauthorized access to Information Systems that contain Restricted Information, and (iii) protecting Restricted Information from being modified without detection, in all three cases as determined appropriate by the CISO.

IV. Procedures

1. Information System Owners will establish and document technical procedures ensuring the integrity for each Information System under their control.

2. Information Systems will be secured in the manner set by the CISO (i.e. information security standards). The CISO will ensure information security standards are available to Information System Owners and IT Custodians.

3. Information System Owners and IT Custodians will establish and document technical procedures that align with the Risk Based Controls defined below and applicable information security standards. This includes documentation that describes the security controls that protect the integrity of their Information Systems.
    a. Information System Owners and IT Custodians will consult with the CISO as needed to create the procedures that achieve these goals. The procedures will include regular monitoring, swift response to unauthorized activities and flaws within the Information System, that takes into account:
        1. Risk assessments
        2. Availability of a solution from the Information System vendor or other third party,

3. The availability of alternatives to address situations and manage risk,
4. The appropriate amount of time to implement the solutions, and
5. Downstream effect on other related systems and imperative workflows.

b. The CISO will provide supplemental guidance on the appropriate timing to implement the solutions and other expectations in light of best practices. At a minimum, Information System Owners and IT Custodians will incorporate the following:

1. Ensure that flaws within Information Systems that could introduce security risks or incidents are addressed in a timely manner.
2. Ensure antivirus technologies are implemented on their Information Systems, as practicable.
3. Monitor their systems for unusual and unauthorized activity. Upon reasonable belief of unauthorized activity, the Information System Owner, or IT Custodian, will alert the CISO.
4. Ensure that web-based and Internet facing Information Systems are protected through the use of advanced controls, e.g. web application firewall technologies.
5. Ensure custom developed Information Systems that store, process or transmit Restricted Information follow secure development practices, leveraging industry best practices, sufficient to meet the controls below.

IV. 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.

System and Information Protection Integrity Procedures (SI-1 C)	
Core	The CISO establishes security standards applicable to the (i) management of Information System flaws, (ii) reducing impact of malicious code, and (iii) management of Information System security alerts. Each Information System Owner, or their delegate, establishes technical procedures that meet these security standards.
Low	N/A
Moderate	N/A
Flaw Remediation (SI-2 CM)	
Core	Where practicable, technical procedures will account for the following: a. Identification, reporting and correction of flaws b. Testing of software and firmware updates for effectiveness prior to installation in a production environment c. Installing security-relevant software and firmware updates

	d. Incorporating flaw remediation into the configuration management process. Examples of this type of activity include: patching security vulnerabilities within operating systems or third party software (such as Adobe Flash or Adobe Acrobat), testing and installing service packs after continuity testing has been competed, and responding to flaws discovered from vulnerability scans (such as host based or web application vulnerability scanning processes).
Low	N/A
Moderate	A vulnerability management program is operated by IT Security in an automated manner to continuously determine the state of the College's Information Systems. This program will be executed at least on a monthly basis.
Malicious Code Protection (SI-3 CM)	
Core	Where practicable, Information Systems will be configured with antivirus software that continuously checks for malicious code running or stored on the system. Updates to the antivirus must occur on, at least, a daily basis. Antivirus will be configured to: a. Perform periodic scans on the Information System on a regularly defined schedule, preferably once a week; b. Automatically block the malicious code, if detected, and send an alert to IT Custodian.
Low	N/A
Moderate	Antivirus systems on the College's Information Systems will be centrally managed. This central management will include the following activities: a. Planning, implementing, accessing, authorizing, and monitoring the effectiveness of the controls; b. Automatic updating of the antivirus detection engines, as well as definition files, to provide the latest threat protection.
Information System Monitoring (SI-4 CM)	
Core	Information Systems will: a. Be monitored for any indicators of attack, such as unauthorized local, network or remote connections. b. Be configured to monitor for unauthorized use or abuse by users of the system c. Be configured to protect log information from unauthorized access or modification

Low	N/A
Moderate	Where practicable, Information Systems will: a. Be configured to send log information to the IT Security Office, in real-time, for consumption within their Security Information and Event Management (SIEM) system. b. Be configured to monitor inbound and outbound communications for unusual or unauthorized activities. c. Be configured to send system alerts to Information System Owners upon indication of compromise, or potential for compromise. In the event of such an alert, and with reasonable assumption of compromise, the Information System Owner will notify the IT Security Office and take direction in accordance with their Incident Response procedures.
Security Alerts, Advisories, and Directives (SI-5 C)	
Core	The IT Security Office will: a. Subscribe to, receive and process security alerts, advisories and directives from external sources, such as US-CERT, the Incident Command Center, or the appropriate ISAC b. Generate and communicate appropriate alerts to Information System Owners, and other key stakeholders, upon the event of an actionable and critical information c. Upon the determination of critical advisories, monitor Information System Owners for the successful remediation activities provided within the advisory. If remediation is unsuccessful, or not implemented according to the appropriate time frame, the IT Security Office will escalate as appropriate.
Low	N/A
Moderate	N/A
Software, Firmware and Information Integrity (SI-7 M)	
Core	N/A
Low	N/A
Moderate	The Information System will be configured with integrity verification tools to detect unauthorized changes to its software, hardware, or operating system. These tools will be configured to detect these changes at startup and at regularly defined frequencies, as defined by the Information System Owner. Unauthorized changes will be delivered, in real-time, to the IT Custodian and the IT Security Office and will abide by the appropriate Incident Response procedure.

Spam Protection (SI-8 C)	
Core	The IT Services will be responsible for managing email servers and deploying anti-spam technologies to detect and block unsolicited messages. Updates to the anti-spam technologies must be conducted on a daily basis, in an automated manner.
Low	N/A
Moderate	N/A
Information Input Validation (SI-10 M)	
Core	N/A
Low	N/A
Moderate	The Information System will be configured to check the validity of inputs through its various communication channels, such as web-based services and client-server based communications. These inputs will be sanitized, by validating the syntax and semantics of the information being inputted, to prevent input- corruption based attacks such as SQL Injection or Cross-Site Scripting.
Error Handling (SI-11 M)	
Core	N/A
Low	N/A
Moderate	The Information System will be configured to generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries. These error messages will only be accessible to Information System Owners, IT Custodians, or the IT Security Office. For example, the Information System will be prohibited from generating actual passwords used in a failed login attempt. Additionally, it will be configured to not take automated action upon the content of the error message, which could introduce activation of malicious scripts through the error handling process.
Memory Protection (SI-16 M)	
Core	N/A
Low	N/A
Moderate	The Information System will be configured to protect its memory from unauthorized execution. Examples of memory protection include data execution prevention technologies and address space layout randomization.

VI. Interpretation, Implementation and Revision

The CISO, with the support of IT Custodians and the Office of General Counsel, is responsible

for the interpretation and implementation of this policy and recommending revisions of this policy to the College.

Systems and Communication Policy

I. Purpose

This policy is an element of the College's Security and Privacy Policies. It sets forth sets forth the general framework for how Information Systems will be configured to communicate, and the protections that must be in place in order to ensure the security of those communications.

II. Scope

This policy applies to all Information Systems used to store, process and transmit the College's information. All Covered Individuals are subject to this policy.

III. Policy

The College's CISO determines the security standards under which all Information Systems will operate. Security controls implemented will be based upon the Security Obligations and will focus on communication mechanisms that enable information to be received by, and transmitted from, Information Systems.

This policy supports the College's goal of corroborating that Restricted Information has not been altered, modified or destroyed in an unauthorized manner, guards against unauthorized access to Restricted Information that is being transmitted over an electronic communications network, and requires encryption of Restricted Information during transmission, where appropriate as determined by the CISO.

IV. Procedures

1. Information System Owners are responsible for identifying IT Custodians (i) for each Information System under their control, and (ii) for the operations of the network and firewalls in which the Information System resides.
2. Information Systems will be secured in the manner set by the University CISO (i.e. information security standards). The CISO will ensure information security standards are available to Information System Owners and IT Custodians.
3. Information System Owners and IT Custodians will establish and document technical procedures that align with the Risk Based controls defined below and applicable information security standards. This includes documentation that describes the inbound and outbound connections to the Information System.
4. Information System Owners and IT Custodians will implement the technical procedures and will routinely check to ensure configurations are working as intended.
5. Information System Owner will report to the CISO (i) the failure of security configurations or (ii) when information security standards cannot be applied.
6. The CISO, or their delegate, is responsible for:
    a. Reviewing and approving point to point network connections with third parties.
    b. Approving and logging perimeter and data center firewall changes that permit the

communication between Information Systems.

c. Advising, reviewing, approving, and monitoring the security capabilities of the network to limit potentially malicious activity from impacting the College's Information Systems and networks.

7. The CISO may suspend the ability for an Information System to communicate electronically due to extenuating circumstances (i.e. cyber security Incident) and cyber security risks.

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.

System and Communications Protection (SC-1 C)	
Core	The University CISO establishes security standards applicable to the communications that occur between Information Systems. Each Information System Owner, or their delegate, establishes technical procedures that meet these security standards.
Low	N/A
Moderate	N/A
Application Partitioning (SC-2 M)	
Core	N/A
Low	N/A
Moderate	Applications residing on Information Systems will partition their user-based functionality from the information system management based functionality. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls. Examples include ensuring that the same method for administrating databases, network components and server configurations are not used by general users.
Information In Shared Resources (SC-4 M)	
Core	N/A
Low	N/A
Moderate	The Information System is configured to prevent unauthorized or unintended information transfer via shared system resources. This is commonly referred to as "object reuse" and "residual information protection". This prevents the ability for information leveraged by prior users (or processes) of the system to be accessible by current users (or processes) of the system when said objects exist on shared resources such as main memory, registers and hard disks.
Denial of Service Protection (SC-5 L)	
Core	N/A

Low	The Information System is configured to protect against or limit the effects of denial of service attacks. This will include, but is not limited to, attacks such as SYN/ACK flooding, ICMP ping floods, SMURF attacks, DNS amplification attacks, resource exhaustion attacks, and others. Employing both access list restrictions on the Information Systems, or ensuring that the Information Systems are protected by the appropriate firewalls will assist with application of this control.
Moderate	N/A
Boundary Protection (SC-7 CLM)	
Core	Publicly accessible components of the Information System will be separated from the internal organizational network by placing these components within a designated network (i.e. "DMZ" or "perimeter network"). Connections between external components and internal components will be managed in such a way that limits the access to only those communication protocols necessary for the function of the external facing component of the Information Systems. Information Systems will be monitored across both external (Internet) boundaries, as well as internal (data center) boundaries.
Low	DMZ protections will include the following: • Prevention of spoofing attacks, such as impersonating an internal IP address when sourced from the Internet. • Firewalls used to segment between the Internet, DMZ, and internal network segments. • Intrusion Prevention Systems and/or Intrusion Detection Systems to detect cyber-attacks targeted against publicly facing Information Systems. • Web Application Firewalls to protect the web based components of publicly accessible Information Systems.
Moderate	The following additional protections will include: • The number of external network connections will be limited to the Information System. • For Telecommunications: o Separate managed interfaces for each external telecommunications service o Established traffic flow policy for each managed interface o Protections of confidentiality and integrity of information flowing across each interface • Exceptions to the traffic flow policy documented
	o Reviews of exceptions to the traffic flow policy on an annual basis

	and immediate removal when the exception is no longer needed. • Firewalls are configured to deny-all communication protocols and only permit appropriate traffic based on an exception basis. The CISO, or their delegate, only can grant this exception. Remote access connections leveraging Virtual Private Network technologies will not be permitted to use split-tunneling techniques. If the Information System detects split-tunneling techniques, it will reject the network communication.
Transmission Confidentiality and Integrity (SC-8 CM)	
Core	The Information System protects the confidentiality and integrity of its transmitted information. Information Systems communicating on external and public networks will disallow insecure network connections when transmitting sensitive information, such as passwords, authentication tokens, session tokens, sensitive business data, or other information that could lead to a compromise of the Information System. Information Systems communicating only on internal networks may employ the same techniques for protecting the communications. In the case where such protections cannot be accomplished, the physical or logical segmentation of the Information Systems communicating amongst one another will be achieved to limit the exposure of insecure network connections.
Low	N/A
Moderate	The Information System will leverage cryptographic methods to prevent the disclosure of information, as well as to detect any unauthorized changes to the information during its transmission.
Network Disconnect (SC-10 M)	
Core	N/A
Low	N/A
Moderate	Technical controls will be established to terminate a network connection associated with a communication sessions at the end of the session, or after 60 minutes of inactivity. For example, a VPN connection will end its session after 60 minutes of inactivity from its connected user, or after a patient logs out of the patient portal the TCP/IP session will immediately deconstruct.
Trusted Path (SC-11 C)	
Core	Information Systems will be configured to establish trusted communications between the users and the Information Systems security components, such as authentication. These paths will be generated in a manner that protects the communications from modification or disclosure.
Low	N/A
Moderate	N/A

Cryptographic Key Establishment and Management (SC-12 C)	
Core	When cryptography is required and used within an Information System, documented procedures must be implemented effectively for cryptographic key generation, distribution, storage, use, and destruction.
Low	N/A
Moderate	N/A
Collaborative Computing Devices (SC-15 CM)	
Core	When leveraging collaborative computing devices, such as electronic networked whiteboards, conference bridges with collaboration tools, and microphones, the devices will: • Prohibit network-based activation without explicit authorization from the Information System Owner, or their delegate, and in such cases with an appropriate activation code. Provide explicit indication of its use to those physically present at the device (such as indications that network based whiteboards are active, or lights indicating an active conference bridge).
Low	N/A
Moderate	Collaboration computing devices are prohibited in Designated Secure Computing Facilities.
Transmission of Security Attributes (SC-16 M)	
Core	N/A
Low	N/A
Moderate	When sharing authentication identification (such as usernames) between Information Systems, the sharing of such information will be protected to ensure that the integrity of the data may not be compromised.
Public Key Infrastructure Certificates (SC-17 L)	
Core	N/A
Low	Information Systems will leverage public key certificates that have been issued by the University of Chicago or University of Chicago Medicine approved certificate authority. The respective Information Security Office will handle requests for public key certificates.
Moderate	N/A
Mobile Code (SC-18 M)	
Core	N/A
Low	N/A
Moderate	Information System Owners must implement controls and procedures for mobile code (e.g. JavaScript, ActiveX, PDF, Shockwave, Flash, etc.) in accordance with NIST SP 800-28. The Information System Owner shall:

	• Define acceptable and unacceptable mobile code and mobile code technologies; • Establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and Authorize, monitor, and control the use of the mobile code.
Voice Over Internet Protocol (SC-19 M)	
Core	N/A
Low	N/A
Moderate	When VoIP is implemented within an Information System, the Information System Owner must establish usage restrictions and implementation guidance for its use. Information Systems that leverage VoIP must be authorized by the CISO and be monitored appropriately.
Secure Name / Address Resolution Service (Authoritative Source) (SC-20 L)	
Core	N/A
Low	Information Systems that provide name or address resolution service (e.g. DNS or WINS) must provide data origin authentication and integrity verification artifacts along with the authoritative name resolution data returned in response to resolution queries. In addition, Information Systems will provide a means of indicating the security states of child zones and enable the verification of the chain of trust between parent and child domains. The most practical use of such a resolution service is the DNSSEC name resolution system, whereby digital signatures and cryptographic keys are used to validate the authenticity of authoritative name servers.
Moderate	N/A
Secure Name / Address Resolution Service (Recursive or Caching Resolver) (SC-21 L)	
Core	N/A
Low	Each client of a name resolution request must request and perform data origin authentication and data integrity verification on the name/address resolution responses received from authoritative sources. DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to enable clients to verify the authenticity and integrity of response data.
Moderate	N/A
Architecture and Provisioning for Name / Address Resolution Service (SC-22 CL)	
Core	The Information System that provides name/address resolution service for the College is designed and implemented to be fault tolerant.

Low	The Information System that provides name/address resolution service for the College will be implemented so as to have an internal role and an external role, such as through the split-DNS architectural design. To prevent network topology information leakage, external DNS servers that host authoritative records for DMZ servers will not contain DNS records for internal servers.
Moderate	N/A
Session Authenticity (SC-23 LM)	
Core	N/A
Low	Information Systems will protect the authenticity of communication sessions. For example, security configurations will be leveraged to prevent man-in-the-middle attacks or session hijacking, or the insertion of false information into an authenticated session.
Moderate	The Information System will: • Invalidate session identifiers upon a user logout or a session termination. • Generate a unique session identifier for each session and recognize only session identifiers that are system generated.
Protection of Information at Rest (SC-28 CM)	
Core	Information Systems must protect information at rest in accordance with the sensitivity of the information being stored.
Low	N/A
Moderate	The Information System will protect the confidentiality and integrity of information classified as Restricted. The following controls will be considered when selecting the protection criteria: • Network segmentation through the use of firewalls • Intrusion prevention / detection systems • Data loss prevention • Access control • Cryptographic controls (encryption)
Process Isolation (SC-39 L)	
Core	N/A
Low	The Information System will maintain separate execution domains for executing processes.
Moderate	N/A

VI. Interpretation, Implementation and Revision

The CISO, with the support of IT Custodians and the Office of General Counsel, is responsible for the interpretation and implementation of this policy and recommending revisions of this

policy to the College.

FCIM Server Room Access Policies and Procedures

I. Purpose

This policy is an element of the College's Security and Privacy Policies. The FCIM Server Room provides stable environments, enhanced security, fire suppression equipment and alarms, uninterrupted power (UPS and generators), high- speed network connectivity and other features required by the mission-critical resources they contain. The policies and procedures described in this document have been developed to maintain a secure, safe environment and must be followed by individuals working in or visiting the Server Room. All individuals requesting access or maintaining servers in the Server Room must understand and agree to these procedures.

II. Overview

The FCIM Server Room contains the College's enterprise computing and networking resources. Access is controlled to protect both the physical resources and the enterprise data from unauthorized use, accidental or malicious damage and theft. Access to the Server Room will only be granted when a legitimate business need is demonstrated. This access policy and procedure document specifies the criteria for granting access to specific individuals or groups. Failure to follow these policies is considered grounds for dismissal and/or prosecution. Failure of a vendor, consultant, or contractor to follow these policies is grounds for termination of agreements and subsequent legal action. Any questions regarding policies and procedures should be addressed to the CISO. This Server Room Access Policy may be suspended in the event of an emergency that requires access for medical, fire, or police personnel.

III. Server Room Access

Unsupervised access to the Server Room is by default reserved only for the IT Custodian and will only be given to other individuals with an approved and demonstrated business need to access the Server Room on a regular basis; those individuals requiring infrequent access will be granted escorted access as needed at the discretion of the CISO. Individuals with unescorted access may escort and supervise unauthorized individuals provided all individuals are logged on entry and exit. Identification belonging to authorized individuals may not be loaned to unauthorized individuals; such action is grounds for disciplinary action. There are no temporary or 'blank' access cards available.

Violations of this policy can result in removal of access. Individuals that violate the policies and are removed from access may face additional disciplinary actions, pending review by the CISO and FCIM Administration.

IV. Server Room Access --- Levels of Access

A. Escorted

Individuals that have an infrequent need for Server Room access will be granted Escorted status only. Escorted access will be provided primarily during normal business hours, while after-hours escorted access will be provided on an emergency or pre-arranged basis only. Individuals requesting escorted access must be signed in and out in the Server Room access log by a member of the FCIM Administration. They are required to provide identification on demand and leave

the facility when requested to do so. They must not allow any other person access to the Server Room.

B. Unescorted
Employees that work inside the Server Room and other individuals that have been granted the access based on their job requirements and a demonstrated legitimate business need will have 24/7 access to the Server Room. FCIM-badged access cards must be visible at all times when in the Server Room.

C. Vendor
Vendors approved by CISO may be granted unescorted access to the Server Room to perform scheduled maintenance or repair work. Vendors not approved for unescorted access may be granted escorted access.

D. Maintenance and Custodial Staff
College maintenance and custodial staff will need to be escorted when accessing the Server Room. All maintenance/custodial staff must sign the access log upon entering and leaving the Server Room and inform the CISO of any maintenance work. The CISO must enter any maintenance work in the operations log.

E. First Responders
Campus first responders are granted unescorted access for emergency situations and pre-arranged visits.

V. Periodic Review and Termination of Access
The CISO will review the access list every 90 days and will remove any individuals who no longer have a legitimate business need to access the Server Room. Any departing employee of the College will immediately be removed from any and all access to the Server Room upon his/her departure.

VI. Server Room Access Log
The Access logs in the Server Room must be maintained at all times by the CISO. All escorted individuals entering the Server Room must sign the log as they enter and exit for audit purposes.

VII. Access Exception Reporting
Any unauthorized access to the Server Room must be, upon discovery by any member of the College's staff, logged by such staff member in the daily operations log and must be reported to the CISO who will determine if the incident needs to be further investigated and/or reported to law enforcement.

Attempts to forcibly enter the Server Room must be immediately reported to law enforcement.

VIII. Server Room Etiquette Rules
It is mandatory that all people working within the Server Room adhere to the posted rules of etiquette. This will insure Server Room safety and efficiency.

IX. Interpretation, Implementation and Revision

The CISO, with the support of IT Custodians and the Office of General Counsel, is responsible for the interpretation and implementation of this policy and recommending revisions of this policy to the College.

Appendix A: Server Room Access Agreement

Name of Applicant Requesting Access: _____

Contact Telephone: _____ Contact Email: _____

Supervisor Name: _____

Access Requested: Unescorted ____ Escorted ____ Maintenance ____

Those granted Server Room access must abide by the following rules:

- FCIM-badged identification (including visitor badges for third party vendors) must be worn visibly at all times.
- Individuals must not touch equipment or supplies belonging to other departments.
- Access must not be used to allow any unauthorized person into the Server Room.
- An individual that has access **MUST** formally log in and out **ALL** visitors that are accompanying them into the Server Room.
- Individuals with access privilege must abide by all policies and procedures as described herein.
- Violating these rules can result in Server Room access being revoked and/or disciplinary action. .
- Read and abide all Server Room access policies and procedures.

I fully understand and agree to these rules. I also agree to provide my full cooperation during any investigation concerning a security matter, which might have occurred in the Server Room during a time when my presence in the facility has been recorded.

Abuse of this access privilege and/or non-compliance with this agreement may result in removal of access and/or disciplinary action.

Applicant's Signature: _____

CISO Name: _____

CISO Signature: _____ Date: _____

Appendix B: Server Room Unescorted Access Request Procedure

1. Each employee requesting unescorted access to the Server Room must complete a *Server Room Access Agreement* form.

2. The CISO must sign the Access Agreement form before it becomes effective.

3. The CISO will review all access requests. The applicant will be notified of the decision by email.

4. All submitted Server Room Access Agreement forms will be filed with the CISO.

5. If the Access Request form indicates an access request to more than one Server Room, the access requests will be evaluated and authorized separately.

6. An employee's supervisor may appeal a denial of access via email to the CISO. The email should include an expanded explanation for the employee access requirements. The decision of the CISO is final.

Appendix C: Server Room Etiquette

1. All work areas must be kept clean and free of debris. Staff performing work in the Server Room must ensure that they have left the areas as clean as they were before beginning their work.

2. To reduce fire hazards rack enclosures must be kept neat and free of manuals, media, boxes and unused equipment. Rack enclosures are not storage cabinets and must only be used for functioning equipment.

3. Doors on all racks should remain closed at all times except during maintenance.

4. Cables should never be strung outside of rack enclosures. Cabling between rack enclosures of adjacent racks is accepted provided sufficient pass-through chassis are in place.

5. Under no circumstances should any person accessing the Server Room:
    a. Lift floor tiles without prior knowledge, consent, and oversight of the CISO.
    b. Tamper with or interfere with the normal function of the sockets, cables, transformers or power distribution units .
    c. Tamper with or interfere with the normal function of the air conditioning units.
    d. Removing any cables or power connections from equipment other than those covered by your SLA.
6. Under no circumstance should any food and beverages of any kind be within the Server Room.

Appendix D: Server Room Approved Vendor Access Procedure

1. Each member of a vendor's maintenance team granted unescorted access to the Server Room must display the FCIM-badged visitor identification card issued for that individual. Sharing identification card is strictly prohibited.
2. Each individual vendor requesting unescorted access to the Server Room must complete the Server Room Access Agreement set forth in Appendix A of this policy. The agreement must be counter-signed by the CISO to be effective.
3. The CISO will evaluate and authorize the request if there is a legitimate business need. In the event that the request is denied, the vendor will be informed by email.
4. After approval of the access request, the access agreement form will be filed with the CISO and the vendor will be authorized for Server Room access.

Incident Response Policy

I. Purpose

This policy is an element of the College's Security and Privacy Policies. It formalizes the requirements for reporting and responding to information security incidents. It serves to minimize the negative consequences of incidents and to improve the University's ability to promptly restore operations affected by such incidents. It ensures incidents are promptly reported to the appropriate officials, that they are consistently and adequately responded to, and that serious incidents are properly monitored.

The CISO is authorized to secure College resources that are actively threatened. When possible, the CISO will abide by this standard and the Incident Response Plan to mitigate the threat. In an urgent situation requiring immediate action and leaving no time for collaboration, the CISO is authorized under the Policy to disconnect any affected device from the network, and to assess vulnerabilities and verify safeguards of College resources.

II. Definitions

An *incident* is defined as an attempted or successful unauthorized access, use, disclosure, modification or destruction of information; interference with information technology operation; or violation of explicit or implied acceptable usage policy. Examples of incidents include (but are not limited to):

- Unauthorized access of systems or data
- Inappropriate usage of systems or data
- Unauthorized change to computer or software
- Loss or theft of equipment used to store personal information or confidential university data
- Unwanted disruption or denial of service
- Interference with the intended use of College resources
- Compromised user account

While this definition covers numerous potential and actual incidents, the requirement for central incident reporting is aimed at serious incidents as defined below.

A *serious incident* is an incident that may pose a threat to College resources, stakeholders, and/or services. Specifically, an incident is designated as serious if it meets one or more of the following criteria:

- Involves potential unauthorized disclosure, modification or destruction of personal information (as defined below)
- Involves serious legal issues
- Causes severe disruption to critical services
- Involves active threats
- Is widespread, that is, extends beyond a single unit
- Is likely to raise public interest

Personal information is defined as a person's first name or first initial and last name in combination with any one or more of the following data elements:

- The person's Social Security Number

- The person's driver license number or non-operating identification license
- The person's financial account number or credit or debit card number in combination with any required security code, access code or password that would permit access to the person's financial account

III. Roles and Responsibilities

The College's staff members have the following primary roles and responsibilities in connection with incidents:

1. Users of College resources

- Promptly report actual or suspected incidents to a local support provider.
- If the local support provider is unavailable, unwilling or unable to correct an incident, disconnect any affected device's network connection (the Ethernet cable but not the power supply) and report the incident to the CISO. In addition, if the incident involves –
    - suspected unauthorized access, theft of university computing equipment or information, or another possible crime, also report the incident to law enforcement and to local authorities if it occurred away from the College campus.
    - Personally identifiable health information or human subject research information, also report it to the Privacy Officer.
    - payment cardholder data, also promptly report it to the College's Finance Department.
    - a serious incident, report it to CISO.
- Assist various parties to resolve the incident and help improve practices and prevent or minimize the occurrence of such incidents in the future.
- In the course of reporting, tracking, and responding to an incident, protect and keep confidential any confidential information or personal information.

2. Local Support Provider

- Promptly report all serious incidents reported to or identified by the local support provider to CISO. In addition, if the incident involves –
    - suspected unauthorized access, theft of university computing equipment or information, or another possible crime, also report the incident to law enforcement and to local authorities if it occurred away from the main campus.
    - personally identifiable health information or human subject research information, also report it to the Privacy Officer.
    - payment cardholder data, also report it promptly to the College's Finance Department.
    - a serious incident, report it to the CISO.
- Evaluate and respond to incidents on a timely basis to prevent additional loss of or harm to College resources, in accordance with College policies and procedures, including the Incident Response Plan and the Incident Response Procedures.
- Assist various parties to resolve the incident and help improve practices and prevent or minimize the occurrence of such incidents in the future.
- Following initial reporting and upon performing remedial actions for any serious incident, notify the CISO for accurate closure of the problem report.

- Notify the affected user of remedial steps taken and recommended mitigating activities.
- In the course of reporting, tracking, and responding to an incident, protect and keep confidential any confidential information or personal information.

3. Information Security Liaisons

- Participate in and support establishment of incident response processes, including incident reporting.

4. Security Personnel

- Maintain a problem report or other documentation of the incident.
- Attempt to contact the user or local support provider regarding any discovered or reported
  incident.
- Communicate to the user and the local support provider any actions that need to be taken by them, the reasons for them, the steps required to re-establish service and any relevant technical information about the incident.
- If the user or local support provider is unavailable, unable or unwilling to correct the incident expeditiously, take necessary and appropriate actions to mitigate or remediate in accordance with College policies and procedures, including the Incident Response Plan and the Incident Handling Procedures.
- Initiate escalation procedures to the appropriate office or party as necessary.
- In the course of reporting, tracking, and responding to an incident, protect and keep confidential any confidential information or personal information.

5. CISO

- Coordinate investigation of serious incidents.
- Report serious incidents to the President.
- Activate a Security Incident Response Team, as deemed necessary.
- Convene an ad hoc committee to review any serious incident involving possible acquisition of personal information that may result in breach notification, or possible unauthorized acquisition, access, use or disclosure of personally identifiable health information that may result in breach notification.
- Report findings of fact relevant to the serious incident to the ad hoc committee, if any.
- If a decision is made to notify affected subjects, report the information required to the President and General Counsel.
- Initiate escalation procedures to the appropriate office or party as necessary.
- If a decision is made to notify affected subjects, coordinate the drafting of notification communications with management of the affected unit, approve final version (with any other appropriate party), and ensure that the notification procedures are executed.

6. Ad Hoc Committee

- Review any serious incident that potentially involves unauthorized access to and acquisition of personal information that may result in breach notification.
- Determine, based on findings of fact by the CISO, whether criteria for notification under law or College policy have been met and, if so, determine the means of notification.
- Recommend action based on its deliberations and findings.

- Report findings and recommendations to the President and Genera Counsel.

7. **Management of Affected Unit**
   - If advised by the CISO that the ad hoc committee has recommended action, issue notification communications without unnecessary delay, subject to the needs of law enforcement, in coordination with the CISO.

8. **Privacy Officer**
   - Inform the CISO of reported serious incidents.
   - Investigate any reported incident involving personally identifiable health information or human subject research information.
   - If a decision is made to notify affected subjects of an incident involving personally identifiable health information, coordinate the drafting of notification communications with management of the affected unit, approve final version (with any other appropriate party), and ensure that the notification procedures are executed.

9. **Finance Department Services**
   - Inform the CISO of reported serious incidents.
   - Initiate escalation procedures to the College's acquiring bank, member bank and card company, as necessary.

IV. Interpretation, Implementation and Revision

The CISO, with the support of IT Custodians and the Office of General Counsel, is responsible for the interpretation and implementation of this policy and recommending revisions of this policy to the College.

Incident Response Plan

I. Purpose

This policy is an element of the College's Security and Privacy Policies. All authorized users have an interest in the security of College resources at FCIM, and share in the responsibility for protection of those resources, prevention of problems, and incident detection and response. The purpose of this plan is to describe the general procedures that will be followed in response to those *incidents* involving *university resource* that rise to the level of *serious incidents*. A *serious incident* is an attempted or successful unauthorized access, use, disclosure, modification or destruction of information; interference with information technology operation; or violation of explicit or implied acceptable usage policy that may pose a threat to College resources, stakeholders, and/or services. Specifically, an incident is a *serious incident* if it meets one or more of the following criteria:

- Involves potential unauthorized disclosure, modification or destruction of *personal information* (as defined below)
- Involves serious legal issues
- Causes severe disruption to critical services
- Involves active threats
- Is widespread, that is, extends beyond a single unit
- Is likely to raise public interest

Personal information is defined as a person's first name or first initial and last name in combination with any one or more of the following data elements:

- The person's Social Security Number
- The person's Arizona driver license number or non-operating identification license
- The person's financial account number or credit or debit card number in combination with any required security code, access code or password that would permit access to the person's financial account

II. Security Incident Response Team (SIRT)

Serious incidents will be responded to by a specially formed team of individuals led by the CISO – the Security Incident Response Team. This team will be comprised of technical resources with the appropriate skills to identify, assess, respond to and communicate the effects of *serious incidents*. SIRT members will be designated by the CISO, who is authorized to act in the best interest of the College to secure university resources that are actively threatened and to abide by the incident handling procedures to mitigate the threat. Full cooperation with the SIRT is required of all authorized users of university resources.

III. Response to Serious Incidents

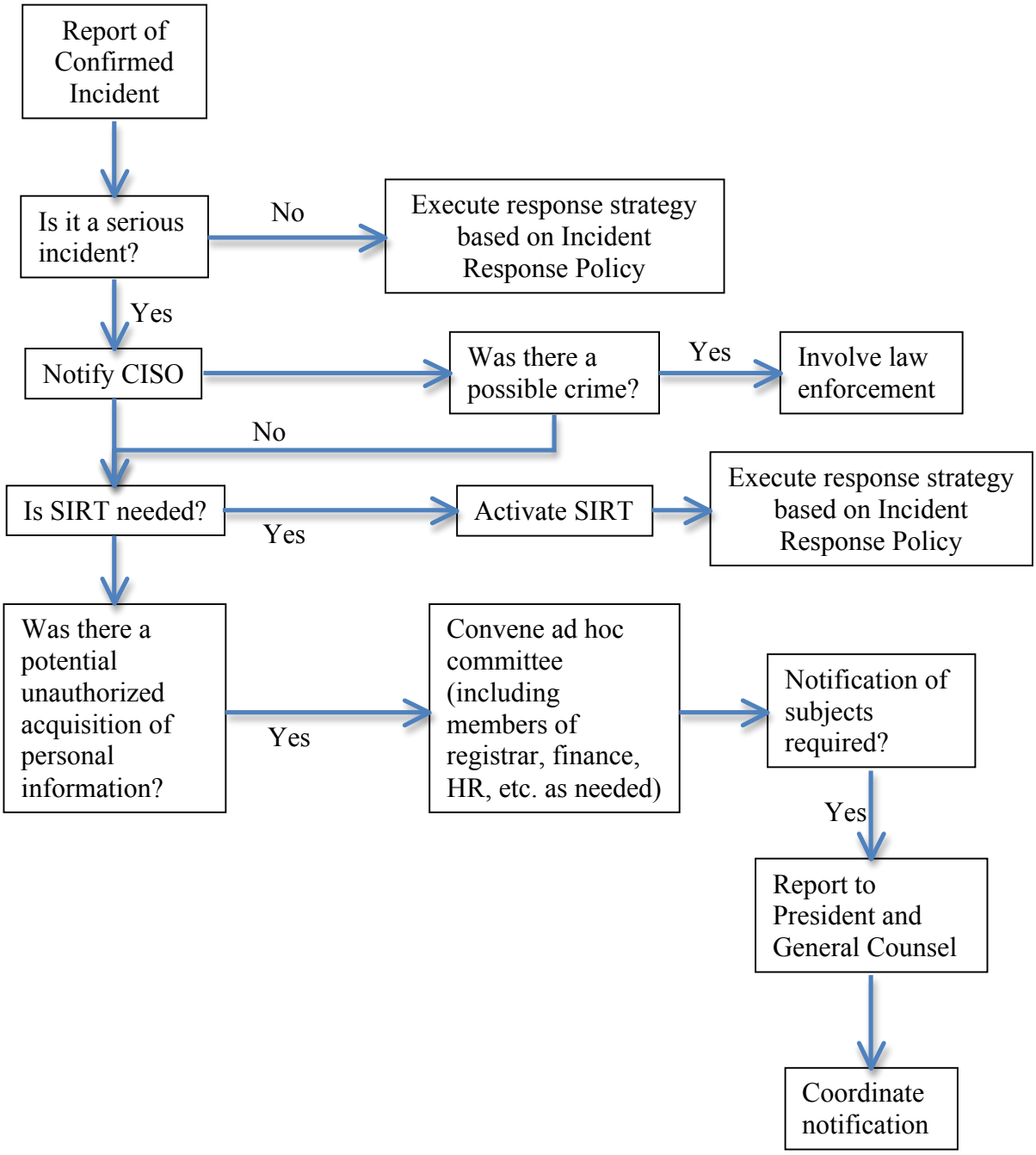
Generally speaking, *serious incidents* will be responded to by containing and eradicating the threat or cause of the problem as soon as possible and as completely as possible while investigative and corrective actions are taken. In addition, appropriate measures to support investigation of the incident will be taken. Cooperation of authorized users with these steps is required. Specifically, procedures will include the practices described in Appendix A to this plan,

as appropriate.

IV. Interpretation, Implementation and Revision

The CISO, with the support of IT Custodians and the Office of General Counsel, is responsible for the interpretation and implementation of this policy and recommending revisions of this policy to the College.

Appendix A


Report of Confirmed Incident
Is it a serious incident?
No
Execute response strategy based on Incident Response Policy
Yes
Notify CISO
Was there a possible crime?
Yes
Involve law enforcement
No
Is SIRT needed?
Yes
Activate SIRT
Execute response strategy based on Incident Response Policy
Was there a potential unauthorized acquisition of personal information?
Yes
Convene ad hoc committee (including members of registrar, finance, HR, etc. as needed)
Notification of subjects required?
Yes
Report to President and General Counsel
Coordinate notification

Incident Handling Procedures

I. Purpose

This policy is an element of the College's Security and Privacy Policies. It sets forth the major steps involved in the initial handling of an incident. Portions of this guideline were adapted from *Computer Security Incident Handling Guide* (NIST Special Pub. 800-61), and references are made to relevant Guide pages and other useful materials.

Note that the actual steps performed may vary based on the type of incident being handled, the nature of individual incidents and the strategies chosen for containment, eradication and recovery. For example, if the handler knows exactly what has happened based on analysis of indications (Detection and Analysis, Step 1.1), there may be no need to perform Steps 1.2 or 1.3 to further research the activity. This guideline provides guidance to handlers on the major steps that should be performed; it does not dictate the exact sequence of steps that should always be followed.

Actions should be coordinated as described in the Incident Response Standard. More than one person may be responsible for the steps described in this guideline.

II Detection and Analysis

1. Determine whether an incident has occurred
    - 1.1. Analyze the precursors and indications
    - 1.2. Look for correlating information
    - 1.3. Perform research, using –
        - 1.3.1. Guide references in Step 2
        - 1.3.2. SANS' Intrusion Detection Cheat Sheets for Linux, http://www.sans.org/score/checklists/ID_Linux.pdf
        - 1.3.3. SANS' Intrusion Detection Cheat Sheets for Windows, http://www.sans.org/score/checklists/ID_Windows.pdf
        - 1.3.4. search engines
        - 1.3.5. knowledge base
        - 1.3.6. SANS Incident Identification Form for recording basic info, http://www.sans.org/score/incidentforms/IH_Identification.pdf
    - 1.4. As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence, being careful to ensure that evidence can be preserved, if necessary
2. Classify the incident as:
    - 2.1. Denial of service (Guide at 4-7)
    - 2.2. Malicious code (Guide at 5-5)
    - 2.3. Unauthorized access (Guide at 6-3)
    - 2.4. Inappropriate usage (Guide at 7-3)
    - 2.5. Multiple components (Guide at 8-1)
    - 2.6. Generic, if none of the above (Guide at 3-5)
3. Identify which resources have been affected and forecast which resources will be affected
4. Estimate the current and potential technical effect of the incident
5. Prioritize handling the incident based on the operational impact

III. Reporting

1. Report the incident to the appropriate internal personnel and external organizations, as provided in the Incident Response Standard
2. If reporting to the CISO and/or law enforcement is required, coordinate remaining steps with personnel from such organizations

IV. Containment, Eradication and Recovery

1. Generic Incidents

1.1. Acquire, preserve, secure and document evidence
1.2. Contain the evidence
1.3. Eradicate the incident
1.4. Identify and mitigate all vulnerabilities that were exploited
1.5. Remove malicious code, inappropriate materials, and other components
1.6. Recover from the incident
1.7. Return affected systems to an operationally ready state
1.8. Confirm that the affected systems are functioning normally
1.9. If necessary, implement additional monitoring to look for future related activity

Resources: Guide at 3-17

2. Denial of Service Incidents

2.1. Acquire, preserve, secure, and document evidence
2.2. Contain the incident—halt the denial of service if it has not already stopped
2.2.1. Identify and mitigate all vulnerabilities that were used
2.2.2. If not yet contained, implement filtering based on the characteristics of the attack, if feasible
2.2.3. If not yet contained, contact the Internet service provider for assistance in filtering the attack
2.2.4. If not yet contained, relocate the target
2.3. Eradicate the incident; if Step 2.2.1 was not performed, identify and mitigate all vulnerabilities that were used
2.4. Recover from the incident
2.4.2. Return affected systems to an operationally ready state
2.4.3. Confirm that the affected systems are functioning normally
2.4.4. If necessary and feasible, implement additional monitoring to look for future related activity

3. Malicious Code Incidents

3.1. Contain the incident
3.1.1. Identify infected systems
3.1.2. Disconnect infected systems from the network
3.1.3. Mitigate vulnerabilities that were exploited by the malicious code 3.1.4. If necessary, block the transmission mechanisms for the malicious code

3.2. Eradicate the incident
3.3. Disinfect, quarantine, delete, and replace infected files
3.4. Mitigate the exploited vulnerabilities for other hosts within the unit and/or the university
3.5. Recover from the incident
3.5.1. Confirm that the affected systems are functioning normally

4. Unauthorized Access Incidents

4.1. Perform an initial containment of the incident
4.2. Acquire, preserve, secure, and document evidence
4.3. Confirm the containment of the incident
4.3.1. Further analyze the incident and determine if containment was sufficient (including checking other systems for signs of intrusion)
4.3.2. Implement additional containment measures if necessary
4.4. Eradicate the incident
4.4.1. Identify and mitigate all vulnerabilities that were exploited 4.4.2. Remove components of the incident from systems
4.5. Recover from the incident
4.5.1. Return affected systems to an operationally ready state 4.5.2. Confirm that the affected systems are functioning normally
4.5.3. If necessary, implement additional monitoring to look for future related activity

Resources:
Guide at 6-5 (see link in first paragraph)
SANS, Intrusion Detection Cheat Sheets for Linux, http://www.sans.org/score/checklists/ID_Linux.pdf SANS, Intrusion Detection Cheat Sheets for Windows, http://www.sans.org/score/checklists/ID_Windows.pdf
CERT, Steps for Recovering from a UNIX or NT System Compromise, http://www.cert.org/tech_tips/root_compromise.html

5. Inappropriate Usage Incidents

5.1. Acquire, preserve, secure, and document evidence
5.2. If necessary, contain and eradicate the incident (e.g., remove inappropriate materials)

Resource: Guide at 7-5

6. Multiple Component Incidents

6.1. Follow the Containment, Eradication, and Recovery steps for each component, based on the results of Detection and Analysis

Resource: Guide at 8-2

7. Post Incident Activity

7.1. Create a follow-up report
7.2. Hold a lessons-learned meeting (Guide at 3-22)

V. Interpretation, Implementation and Revision

The CISO, with the support of IT Custodians and the Office of General Counsel, is responsible for the interpretation and implementation of this policy and recommending revisions of this policy to the College.