SAINT MARY'S COLLEGE of CALIFORNIA

Saint Mary's College of California
Institutional Information Security Policy

Revised 2017

1.0. General Policy Statement

College information and data, whether maintained in hard copy (i.e. on paper) or electronically on servers, local computers or other electronic devices, are important and valuable assets of Saint Mary's College of California. College information and data may be private, personal and/or confidential, and thus is protected from unauthorized disclosures pursuant to a variety of Federal and State laws, as well as College policies. The disclosure or sharing of confidential information to unauthorized recipients can cause harm to the College and/or members of the College Community, and in some cases, may expose the College and individuals to legal liability. Additionally, if College information resources are tampered with or made unavailable through accidental or malicious actions, it may impair or interrupt the ability of Saint Mary's College to conduct its regular academic and business activities..

The purpose of this policy is to provide a structured approach to securing information and data that is owned or in the custody of the College, and improving the ability of the College to prevent unauthorized access, interference or destruction of these critical information assets. Saint Mary's College of California requires all employees of the College, and calls on members of the College Community in general, to diligently protect our critical information assets and the infrastructure that stores and delivers them, to the best of their ability and in accordance with this Policy. Willful failure to comply with this Policy may subject employees to appropriate disciplinary action.

1.1 Scope

This policy applies to:

- All members of the College Community to the degree noted in the section on Roles and Responsibilities.
- All electronic and printed data and information obtained, created, stored, collected, processed, or distributed by the College, and all networks, computers, servers and any other information systems owned or controlled by Saint Mary's College of California that contain and/or processes data owned or in the custody of Saint Mary's College of California, regardless of the physical location. This includes College information and data that may be in the physical custody of, or

on computers owned by, contracting vendors or individual members of the community.

1.2. Amendments and additions to this Policy and Security Guidelines

Amendments and additions to this Policy and/or any associated Information Security policies and procedures will be adopted as official College Information Security Policy upon approval by the President’s Council. The CTO will take proposed policy changes to the Council of Deans for their comment before transmitting them in final form to the Provost for submission to the President’s Council for approval.

2.0. Roles and Responsibilities

2.1 Chief Technology Officer (CTO)

The CTO is responsible for strategic oversight of the Information Security Program. His primary task is to align Information Security policy and practice with the strategic goals of the College. Working with the Deputy CTO, the ISO and the ITSSC, the CTO will develop both enhancements to the Information Security posture of the College as a part of the IT Roadmap, and proposals to improve this Policy.

2.2 Deputy Chief Technology Officer

The Deputy CTO is responsible for the operational direction of the Information Security Program. He supervises the ISO, network monitoring and the other technical groups inside IT Services that are responsible for Computer and Network security.

2.21 Information Security Officer (ISO)

The ISO is the day-to-day manager of the Information Security Program, and is responsible for the management of the provisions of this policy, including user training, Security Audits, Risk Assessments and the real time technical defenses of the Saint Mary’s network. The ISO also manages investigations of Information Security breech incidents.

2.22. IT Services Security Committee (ITSSC) Internal (to IT Services) Information Security committee chaired by the Deputy CTO and consisting of technical members of the IT Services Staff, and Management.

This committee is responsible for recommending technical solutions to implement this Policy, Security Guidelines and for the general protection of the confidentiality, integrity and availability of the Information assets of the College. This committee may also recommend changes to, or new, IT Security policies and procedures to the CTO.

2.3. General Counsel

Advise the College and the CTO on legal matters arising from College policy and procedures; review, for consistency with this and other applicable College policies, contract language in vendor and supplier agreements designed to address the protection of information where such vendors and suppliers have access to SMC Data in the performance of their contracted work; and participate in the security incident management process where appropriate.

2.4. Public Safety

Public Safety (PS) works with the ISO to investigate and document Information Security Incidents that may involve possible criminal activity. Public Safety will also respond to any outside law enforcement agency that is investigating related criminal activity. PS will be a primary alert contact for intrusion alarm systems protecting ITS secure facilities and will respond to any alarms promptly.

2.5 Office of College Communications (OCC)

The OCC is responsible for official communications to the public and the Saint Mary's Community in the event of a major Information Security Incident.

2.6. Data Stewards

A Data Steward is usually an employee in a leadership position with the College who has the primary responsibility for a particular set of data. For example, the Registrar is the Data Steward of student records and information; the Assistant Vice President for Human Resources is the Data Steward of personnel files and data; the Assistant Vice President for Finance and Controller is the Data Steward of College financial data. A Data Steward is responsible for certain actions in relation to the security of the data they oversee, such as:

- The classification of all data he/she is responsible for into the categories listed in Section 7 of this Policy entitled "Data classifications and rules." The Steward is also responsible for marking this data as to classification and determining any specific ways it is to be handled beyond the requirements of this Policy, including additional specific Information Security Policies, and operational procedures. Any additional specific policies and procedures of this type should be developed in consultation with the ISO and be approved by the ITIS.
- The granting of permissions to Data Users for access to the data he/she is responsible for, and the degree to which a particular Data User may view and modify the data. A Data Steward is accountable for who has access to Covered and Confidential; data. The degree of access the Steward may grant could range from
    - full access to system administrators,
    - to operational access for Data Users who are employees directly involved in the day-to-day use of the data for College business and academic operations,

    - to providing extracts of the data to Data Users who have a need for a limited amount of the data for some specific work objective or process, but not day-to-day need for operational access.
- Ensure that all Data Users of the data under their stewardship are trained in, and understand, the requirements of this Policy and the procedures they must take to make sure that the confidentiality, availability and integrity of College data in their custody is maintained. Additionally, require Data Users who have access to Covered or Confidential Data for administrative purposes to sign the College's Confidentially Agreement at the onset of their use of this data.
- Maintain records of Data Users who have access to the Covered, Confidential or Private information under their stewardship, and the level of permissions (access) they have. IT Services will support this task.
- To the extent that the Covered and Confidential data is a part of a student education record, ensure adherence to the College's FERPA policy.

2.51. Data Users

A Data User is an employee (including student workers and qualified volunteers) of the College, or contracted Third Party or Vendor, who has access to and uses College data in the course of their work. A Data User may or may not have permission to modify that data, depending on the requirements of their work. A Data User is responsible for the protection of the data to which they have access. A Data User is also responsible for certain actions in relation to the security of the data they work with, such as:

- Understanding and adhering to the requirements of this Policy, Data Security Guidelines, any specific policies set by the Data Steward for the data they are working with, and the procedures they must take to make sure that the confidentiality, availability and integrity of College data in their custody is maintained.
- Report actual or suspected data vulnerabilities and security breeches promptly to the Data Steward of the data involved and to the College ISO.

2.6. All members of the Saint Mary's Community:

All members of the community are responsible for cooperating with the Security measures that are in place to protect the confidentiality, integrity and availability of the information assets of the College, and to protect the privacy of any information concerning other members of the community that is not available to the public through the College's public website or other publications. All Community members should promptly report any actual or suspected data vulnerabilities or security breeches they become aware of, including compromises of any personal computing equipment used on campus, or of their Saint Mary's College on-line identity (password, user name, etc.), to the ISO by calling the IT Services Help Desk.

.

3.0. Data Classifications and Rules:

All College Information and data will be classified to ensure sufficient confidentiality, integrity and availability.

3.1. The **Confidentiality** requirement for all data is classified as follows:

3.11. Covered Data: Covered data are personal information about students, faculty and staff that are protected by Federal and State law and regulations. Information in this category requires strong security controls and protection against disclosure to unauthorized persons. This information should also not be subject to unauthorized modification, use, or destruction. Unauthorized access to this information can constitute a breech that requires the College to self-report the incident to the government and to the individual(s) whose information was exposed. Such a breech may lead to both involve the institutional and individual liability. There are particular sets of this information that are contained in SMC records that are "covered", such as:

- Social Security numbers
- Credit Card Numbers or any other Financial Account Numbers
- Driver's License Numbers
- Health Records
- Grades
- Student Records

3.12. Confidential Data: Confidential Data are sensitive information that does not fall under the Covered Data criteria or requirements listed above, but should not be available to unauthorized persons by College policy. Again, this information should not be subject to unauthorized modification or use, interference with availability, or destruction. However, though the sensitivity of this data is less than that of Covered data, some information may be considered highly confidential by the College and require the same protections as Covered data. The types of data that fall under the Confidential classification include but are not limited to:

- Faculty and staff personnel files, benefits information, and personal contact information
- Admission applications
- Donor contact information and non-public gift amounts
- Privileged attorney-client communications and work-product.
- SMC internal email and other communication, non-public reports, budgets, plans, and financial information
- Non-public contracts
- Student and employee ID numbers
- Passwords
- Directory information for students who specifically opt out

3.13. Private Information: Private information is information of a personal nature about students that is not designated as Directory information under FERPA. For faculty and staff, private information is personal information, as opposed to business information, that is not designated as Directory information by HR policy. Private information may be information that does not fall under the above classifications of Covered or Confidential, but should be treated by Data Users and the College Community as confidential, and should not be revealed to persons outside of the College Community unless the public release of such information is agreed to in writing by the individual affected, or where required by government authority or valid subpoena or legal process.

314 Public Information: Information that has no restrictions on dissemination. An example of public information would be maps and direction to and around the campus that appears on the College's main web site. However, security controls are still necessary to protect the availability and integrity of the web files and servers that provide this kind of information to the public and members of the College community when needed.

3.2. The **Availability and Integrity** requirement for all data is classified as follows:

3.21. Critical: Information is considered Critical if the loss, loss of availability or unauthorized modification of it would cause the College to be out of compliance with applicable Federal and/or State law or the requirements of contracts; have a significant adverse impact on the business or finances of the College, or on members of the College Community; or cause embarrassment and damage the reputation of the College.

3.22. Non-Critical: Information is considered Non-Critical if the loss, loss of availability or unauthorized modification of it would cause minor inconvenience to campus users while being recovered, and incur limited recovery costs.

4.0. Acceptable Use

All users of the information resources of Saint Mary's College, including networks, computers, accounts, software and storage, are bound by the *Saint Mary's College of California Technology Use Policy*. Use of Covered, Confidential or Private information is strictly limited to job-related tasks.

5.0. Access

Access to Covered, Confidential or private information is on a need-to-know basis. Access to this information and the systems that store it is limited to authorized employees or contractors who need access in the performance of their job duties or related tasks.

- System privileges shall be configured to give Data Users access only to that portion of this data that is needed for the purposes for which they are authorized, and logs of that access must be kept.
- In order to prevent unauthorized viewing, Covered, Confidential or Private information shall not be maintained or displayed in plain sight, and must be secured when unattended. Covered, Confidential or Private information must not

be posted on any web site available to anyone but those authorized to view and use the particular information for legitimate business and job related tasks.

- The use of Social Security Numbers in particular must be limited to those circumstances where such use is required for government reporting purposes and compliance with governmental regulation.
- User Names and Passwords must be used to access Covered, Confidential or Private information and must conform to the password requirements stated in Section 3.3.1 Passwords in the *Saint Mary's College of California Technology Use Policy.* Passwords that provide access should never be shared, stored on a computer in an unencrypted format, or displayed on notes or the like left near a computer. In some cases where a high level of access security is required, two factor authentication may be required.
- Confidentiality Agreement: Any Data User who will have access to any Covered, Confidential or Private information or data for administrative purposes must first sign the *Saint Mary's College of California Confidentiality Agreement*, or have signed a departmental confidentiality agreement that pre-dates the adoption of this Policy. Copies of these agreements will be kept by the appropriate Data Steward.
- Separation, termination or retirement. All privileges granted to any Data User to access Covered, Confidential or private information or data must be immediately revoked and removed upon the end of employment.

6.0. Compliance

The management and protection of the information assets of Saint Mary's College of California shall comply with all applicable government regulations, including The **Family Educational Rights and Privacy Act (FERPA),** The **Gramm-Leach-Bliley Act (GLBA), California Civil Code sections 1798.29(a)** (also known as Senate Bill 1386), The California **Identity Theft Protection Act**, and all laws governing Intellectual Property.

7.0. Computer and Network Security

7.1 Passwords: See *Saint Mary's College of California Password Policy.*

7.2. Anti-malware and Patching: All computing equipment attached to the Saint Mary's network must have appropriate anti-malware software installed and active. Additionally, all connected computing equipment must have up-to-date Operating System (OS) and application security patches. The patching of network equipment and servers should be accomplished within the Change Management process (see 7.3 below).

7.3. Change Management: Data and system integrity shall be maintained in part by conducting all changes to enterprise computer and network systems according to a planned and supervised change management process that adheres to industry standard practices.

7.4. System and Network protection; Monitoring: Industry standard measures and best practices, such as the deployment of security equipment (example: firewalls and intrusion prevention/detection devices) and system "hardening" shall be employed by IT Services to protect network and server systems from malicious attack and compromise, both from inside and outside the Campus network border. IT Services shall monitor the campus network and systems "health" using such methods as log collection/analysis to detect malicious activity and penetration testing to detect vulnerabilities to malicious attack or compromise.

- In this context, "monitoring" means the observation of general activity on the network to detect threats to the confidentiality, integrity and availability of the information assets of the College.

8.0. Data and Information Handling

8.1. Data storage

- As a general rule, Covered, Confidential or private data should only be stored on secure and hardened servers, with appropriate access controls, and located in physically secure facilities.
- All paper and electronic media copies of Covered, Confidential or private information must be stored, when not in use, in locked desks or cabinets.
- Hard copies or prints of Covered, Confidential or private information should be made on equipment in physically secure locations and should never be left unattended in any printer or copier.
- Copies of Covered or Confidential data in a digital format should never be stored on portable computer devices or media unless in an encrypted, password-protected format. This includes data stored on a hard drive or similar component in a portable device such as a laptop computer.

8.2. Data Transmission: It is the responsibility of all Data Users to take proper precautions when transmitting or transporting Covered, Confidential or private data from one location to another, whether the data is in electronic or paper format.

- Transmission of Covered, Confidential or Private data over any network should utilize only "trusted" connections using NIST standard encryption methods. Data Users working outside of Campus should only use a secure VPN to connect to the Campus network.
- Email: Covered or Confidential data contained in Email messages must be encrypted. There are a number of methods available to do this when needed, and IT Services will support employees who need help complying with this provision.
- Mail: Transmission of Confidential information using Campus mail must be contained in a sealed envelope marked "Confidential." Transmission of Covered information must be contained in a sealed envelope marked "Confidential," and hand delivered to its recipient. The US mail may also be used for transmission of such information. Transmission of such information via US mail should be sent Certified, with a return receipt.

8.3. Data Backup and Recovery. Industry standard best practice data backup measures must be employed to prevent the loss and ensure the recovery of all essential data owned by the College. The methods employed must be consistent with the needs of Disaster Recovery and Business continuity.

8.4. Destruction of data and disposal of hardware. Covered, Confidential or Private information must be disposed of by means that make later retrieval by unauthorized persons impossible.

- All printed materials that contain Covered, Confidential or Private data shall be shredded before disposal.
- Computing equipment withdrawn or retired from service: All Covered, Confidential or Private data on hard Drives and other devices and/or media that store data must be completely removed or rendered unreadable and irretrievable before disposal.
- Department/Office specific and general records retention schedules and policies must also be applied to Covered, Confidential and Private data as appropriate, consistent with the *Saint Mary's College of California Document Retention and Destruction Policy*.

9.0. Physical Security

All Data Users are responsible for the physical security of any Covered, Confidential or Private information that is in their possession, whether in a hard (paper) format or on electronic media, and should be protected accordingly while in their care.

- All areas where Covered, Confidential or Private data is viewed or processed as a part of regular work shall be separated from publically accessible areas by locked doors (secure areas).
  - Any person who is not authorized to access or view such data shall not be left unattended inside such a secure area.
- All network edge data equipment shall be located inside locked cabinets, closets or rooms. Major data facilities, such as those housing network core elements and server rooms, where Covered, Confidential or private information and data are stored and/or processed, or used for the delivery of critical academic tools and information, shall be locked, with key access limited to the appropriate IT Services and Public Safety personnel, and shall be protected by an appropriate monitored alarm system, with individually issued pass-codes. Monitored alarm systems shall be configured to notify the appropriate IT Services and PS personnel and systems if breeched.
- Computer monitors and other devices that display Covered, Confidential or Private information that is in use by Data Users in the course of their work should be arranged so that unauthorized persons cannot view the displayed information. Unauthorized persons should never be allowed to "look over the shoulder" of a Data User at displays of Covered, Confidential or Private information.
- Any mobile computing equipment and electronic media that contain Covered, Confidential or Private data shall not be left unattended unless properly locked away in a secure location.

10.0. Risk Assessment

The ISO will conduct regular assessments to identify reasonable foreseeable risks to the confidentiality, integrity and availability of the information assets of the College, and evaluate the effectiveness of the policies and measures in place to protect these assets. Recommendations for improvements that arise from the results of these risk assessments will be made to the ITIS.

11.0. Training and Awareness

The ISO will work with the Data Stewards to provide training to Users in the elements of this policy and all associated data security policies and procedures, as well as in good information security practice. Also, to reduce the over-all risk of breech by malicious actors, the ISO shall establish and maintain an Information Security publicity program to raise awareness and to provide all members of the College Community tools, techniques and practices that should be incorporated into their everyday use of data resources and equipment to both protect themselves and the critical information resources of the College

12.0. Information Security Incident Response and Management

Any action or event that breaches this and/or any associated College security Policies, Guidelines and procedures, or adversely affects the confidentiality, integrity or availability of College Information and information assets and resources, shall be treated as an Information Security Incident, and be investigated and documented. Incidents shall be classified minor, serious or critical. Serious and critical incidents, and where the Incident Report recommends further actions and/or controls, will be presented to the ITIS during its next meeting for review and further action if appropriate.

Associated Documents:

Saint Mary's College of California Technology Use Policy and related Policies
Saint Mary's College of California Document Retention and Destruction Policy
Family Education Rights and Privacy Act (FERPA) Policy
Saint Mary's Web Privacy Policy