Saint Mary's College of California
Information Technology Policy

Information
Technology Services

GLBA Compliance Policy

Policy:	No: 3.0
Responsible Officer:	Chief Information Officer, James Johnson
Effective Date:	February 5, 2024
Updated:	February 5, 2024
Issued By:	ITS - Information Technology Services

CONTENTS

Purpose and Benefits: 2
Designate a Qualified Individual: 2
Activities and Practices Affected by GLBA: 3
1. Handling PII (Personally Identifiable Information): 3
2. Managing Financial Information: 3
3. Student Financial Information: 3
Key Points 3
Roles and Responsibilities: 3
1) IT Department: 3
2) Deans and Department Heads: 4
3) Employees with Access to Protected Data: 4
4) Controller's Office: 4
5) External Financial Auditors: 4
6) Compliance Entity: 4
7) Legal Counsel: 4
8) Institution's Leadership: 4
9) Data Custodians: 4
Conduct a Risk Assessment: 5
Design and Implement Safeguards: 5
Regularly Monitor and Test Safeguards: 5

Train Your Staff: 5
Monitor Your Service Providers: 5
Keep Your Information Security Program Current: 6
Create a Written Incident Response Plan: 6
Require Your Qualified Individual to Report to Your Board of Directors: 6
Contact Information 6
Glossary for GLBA and NIST Framework Terms 6
Specific NIST SP 800-53 Control References: 7
Revision History 8

Purpose and Benefits:

The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act, is a federal law enacted in 1999 in the United States. Its primary purpose is to enhance the privacy and security of customers' nonpublic personal information held by financial institutions. Under GLBA, financial institutions are required to establish safeguards to protect this sensitive information from unauthorized access and disclosure.

GLBA applies not only to traditional banks and financial institutions but also to certain educational institutions that meet specific criteria. If a college or university engages in financial activities involving customer information, such as administering financial aid programs, managing student loans, or operating as a financial institution in any capacity, it may be subject to GLBA regulations.

To ensure compliance with GLBA, educational institutions like SMC must integrate specific guidelines from their Information Security Policy with recognized cybersecurity risk management frameworks, such as the one provided by the National Institute of Standards and Technology (NIST). This integration demonstrates the institution's dedication to complying with GLBA by aligning its internal policies with nationally recognized standards. By doing so, SMC strengthens its defenses against cyber threats and ensures the security of sensitive customer information, meeting the legal requirements and protecting the privacy of individuals' financial data. In essence, GLBA mandates that higher education institutions take necessary steps to safeguard financial information, just as traditional financial institutions are required to do.

Designate a Qualified Individual:

1) The Chief Information Officer (CIO) at SMC, in coordination with a virtual CISO, will lead and manage the information security program, aligning with the *NIST SP 800-53* framework (Section 4.2.5 from **SMC Information Security Policy**).

Activities and Practices Affected by GLBA:

1. **Handling PII (Personally Identifiable Information):**
   a. What it is: PII refers to any information that can be used to identify an individual, such as their name, Social Security number, address, or date of birth.
   b. Offices Affected: Various offices across the institution may handle PII, including the Admissions Office, Financial Aid Office, Registrar's Office, and Human Resources.

2. **Managing Financial Information:**
   c. What it is: Financial information encompasses data related to financial transactions, account balances, payment history, and other financial records.
   d. Offices Affected: The Controller's Office, Bursar's Office, and Financial Aid Office are typically involved in managing financial information.

3. **Student Financial Information:**
   e. What it is: Student financial information pertains to records and data associated with students' tuition, fees, financial aid awards, and billing.
   f. Offices Affected: The Financial Aid Office, Bursar's Office, and Registrar's Office are directly responsible for managing student financial information.

Key Points

- The GLBA Compliance Program is a continuous process that is undertaken at periodic intervals.
- IT Security is responsible for implementing this GLBA Compliance Program.
- IT, with the collaboration of HR, develops appropriate training programs to ensure staff are aware of protocols for protecting customer information.
- IT Services, working with responsible units and offices, monitors, evaluates, and adjusts the Compliance Program in light of the results of the risk management process.

Roles and Responsibilities:

1) **IT Department:**
   a. Ensures the security and encryption of electronic data containing PII and financial information.
   b. Implements and maintains firewalls, intrusion detection systems, and other cybersecurity measures.
   c. Monitors network activity for any unauthorized access or breaches.

2) Deans and Department Heads:

a. Collaborate with IT to identify and classify sensitive information within their respective departments.
b. Ensure that staff members with access to sensitive data are trained in data security practices and follow the institution's policies.

3) Employees with Access to Protected Data:

a. Abide by the institution's data security policies and procedures.
b. Handle sensitive data with care and report any suspicious activities or potential breaches promptly.

4) Controller's Office:

a. Oversees the financial records and ensures compliance with GLBA requirements.
b. Works with IT to implement controls for securing financial data.

5) External Financial Auditors:

a. Review the institution's financial practices and records to ensure compliance with GLBA.
b. Confirm that appropriate safeguards are in place to protect sensitive financial information.

6) Compliance Entity:

a. IT Security coordinates and monitors GLBA compliance efforts.
b. Regularly reviews policies and procedures, making necessary updates to maintain compliance.

7) Legal Counsel:

a. Provides legal guidance on GLBA-related matters and data breach reporting requirements.

8) Institution's Leadership:

a. Demonstrates commitment to GLBA compliance and allocates necessary resources for cybersecurity measures and staff training.

9) Data Custodians:

d. Individuals or departments responsible for the custody and control of specific categories of sensitive data ensure data is protected according to established policies and procedures.

Conduct a Risk Assessment:

a. Risk and gap assessments at Saint Mary's College of California are key for ongoing risk management. These evolving documents identify and address organizational issues, aligning with the *NIST Framework: Identify (ID.AM, ID.RA), Protect (PR.AC, PR.DS), Detect (DE.AE, DE.CM), Respond (RS.RP, RS.CO), and Recover (RC.IM, RC.CO*). Regular updates to these assessments are essential, particularly in response to major changes in business processes, software, and infrastructure. This systematic approach ensures comprehensive risk handling. (Sections 4.4 and 4.13).

Design and Implement Safeguards:

a. **Access Controls**: Implementing SMC's access control policies (Section 4.10 and 4.11) in alignment with *NIST SP 800-53 AC-1*.
b. **Data Inventory:** Managing IT assets and classified information (Section 4.6 and 4.5) adhering to *NIST SP 800-53 CM-8*.
c. **Encryption**: Securing data during transit (Section 4.11.8.ii) in line with *NIST SP 800-53 SC-28*.
d. **App Security**: Ensuring application security (Section 4.11) following *NIST SP 800-53 SA-11*.
e. **Multi-Factor Authentication**: Applying multi-factor authentication (Section 4.10) as per *NIST SP 800-53 IA-2*.
f. **Secure Disposal:** Disposing of data securely (Section 4.5) according to NIST SP 800-88.
g. **Change Management:** Managing organizational changes (Section 4.1 and 4.11) consistent with *NIST SP 800-53 CM-3*.
h. **User Activity Monitoring**: Monitoring user activities (Section 4.14) aligning with *NIST SP 800-53 AU-2*.

Regularly Monitor and Test Safeguards:

a. Integrate SMC's vulnerability management and security operations (Sections 4.13 and 4.14) with *NIST SP 800-53 CA-2*.

Train Your Staff:

a. SMC's training approach (Sections 4.7 and 4.11) follows *NIST SP 800-50*.

Monitor Your Service Providers:

a. Align service provider oversight (Sections 4.4 and 4.12) with *NIST SP 800-53 SA-9*.

Keep Your Information Security Program Current:

a. Maintain an up-to-date security program (Section 4.4) in accordance with *NIST SP 800-37*.

Create a Written Incident Response Plan:

a. Develop an incident response plan (Section 4.8) consistent with *NIST SP 800-61*.

Require Your Qualified Individual to Report to Your Board of Directors:

a. The CIO will report security-related matters to the board, adhering to *NIST SP 800-53 PM-9*.

Contact Information

Persons who may have questions regarding the security of any of the categories of information that is handled or maintained by or on behalf of the College may contact:

James Johnson
Chief Information Officer
925-631-8003 x8003
Jhj2@stmarys-ca.edu

Glossary for GLBA and NIST Framework Terms

1) **GLBA (Gramm-Leach-Bliley Act):** A U.S. law that requires financial institutions, including certain educational institutions such as Saint Mary's College of California (SMC), to protect the privacy and security of customer information.

2) **NIST (National Institute of Standards and Technology):** An agency that provides a comprehensive set of guidelines and standards to help organizations manage cybersecurity risks.

3) **CIO (Chief Information Officer)**: The senior executive at SMC responsible for overseeing the information security program in alignment with cybersecurity frameworks like *NIST SP 800-53*.

4) **Virtual CISO (Chief Information Security Officer)**: An outsourced service providing expert guidance and management of an organization's information security program.

5) **SOC (Security Operations Center**): A centralized unit that deals with security issues on an organizational and technical level.

6) **Access Controls**: Security measures that regulate who or what can view or use resources in a computing environment.

7) **Data Inventory**: The process of cataloging and managing IT assets and classified information within an organization.

8) **Encryption**: The method of converting data into a code to prevent unauthorized access, especially during data transmission.

9) **App Security**: Measures and controls that ensure the security of software applications within an organization.

10) **Multi-Factor Authentication (MFA)**: A security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.

11) **Secure Disposal**: The process of destroying data or decommissioning data storage devices to ensure that sensitive information cannot be recovered.

12) **Change Management**: A systematic approach to dealing with the transition or transformation of an organization's goals, processes, or technologies.

13) **User Activity Monitoring**: The process of tracking and monitoring user actions and behavior within a network or system.

14) **Risk Assessment**: The process of identifying, analyzing, and evaluating risks associated with cybersecurity.

15) **Vulnerability Management**: The cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities in software.

16) **Security Program**: A set of policies, procedures, and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems.

17) **Incident Response Plan**: A set of instructions that help IT staff detect, respond to, and recover from network security incidents.

18) **Board of Directors:** The group of individuals elected to represent shareholders and govern the activities of an organization.

Specific *NIST SP 800-53* Control References:

1) *AC-1*: Policies and procedures for managing access to organizational systems and information.

2) *AU-2*: Procedures for monitoring and tracking audit events in information systems.
3) *CA-2*: Security assessments to evaluate the effectiveness of security controls.
4) *CM-3*: Management of changes to systems, applications, and infrastructure to maintain security.
5) *CM-8*: Keeping track of the components of information systems and their inventory.
6) *IA-2*: Processes for identifying and authenticating users accessing systems.
7) *PM-9*: The strategy for managing the organization's risk related to information systems.
8) *SA-9*: Controls for managing external services provided to the organization.

Revision History

This standard shall be subject to periodic review to ensure relevancy.

Date	Description	Reviewer
02/05/2024	Senior Staff	James Johnson
02/06/2024	Publish	James Johnson