MICHIGAN STATE UNIVERSITY

University Policy

POLICY NAME: Gramm-Leach-Bliley Act

POLICY NUMBER:

Authority Title and Review Information:	Name and Date
Approval Authority:	Senior Vice President, Chief Financial Officer and Treasurer
Responsible Executive:	Associate Vice President and University Controller
Responsible Office:	Office of the Controller
Responsible Officer:	Chief Accountant
Policy Category:	Finance
Effective Date:	February 24, 2025
Last Review Date:	June 15, 2018
Next Review Date:	June 1, 2028

Table of Contents

I. POLICY STATEMENT

The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" (GLB Act), includes privacy provisions to protect consumers' personal financial information held by financial institutions. In 2003, the Federal Trade Commission (FTC) confirmed that higher education institutions are considered financial institutions under this federal law. The Safeguards Rule of the GLB Act requires financial institutions to have a security plan to protect confidentiality and integrity of personal information.

Privacy notices explaining an institution's information-sharing practices must also be provided.

II. SCOPE

As of May 23, 2003, colleges and universities must be in compliance with provisions of the GLB Act that relate to the Safeguards Rule. Safeguarding data has two major components: privacy and security. Colleges and universities that already comply with the Family Educational Rights and Privacy Act (FERPA) are deemed to be in compliance with FTC privacy rules under the GLB Act to the extent the information held relates to students. In addition, colleges and universities are subject to the provisions of GLB related to the security of customer information.

While Michigan State University is primarily an educational institution and its areas covered by the GLB Act are few, the University is committed to complying with the law. This site provides detailed information on University policies and procedures designed to facilitate compliance.

Report complaints and potential violations to the MSU Controller's Office.

III. DEFINITIONS

Covered Service Offerings

1. How do I know if a service offering of my unit is covered?

If you engage in offering a financial product or service normally offered by a financial institution, you maintain records (electronically or paper) about the consumers of that service and their transactions, and you are significantly engaged in that offering, you may be required to comply with the GLB Act.

Examples of activities considered to be financial in nature are:

1. Extending credit and servicing loans. For example, student loans, including receiving application information.
2. Providing educational courses, and instructional materials to consumers on individual financial management matters.
3. Providing financial, investment, or economic advisory services.
4. Collection of delinquent loans.
5. Check cashing services.
6. Providing tax-planning and tax-preparation services.
7. Obtaining information from a consumer report.
8. Providing credit counseling services.
9. Career counseling services for those seeking employment in finance, accounting or auditing.
10. Issuing credit cards or long-term payment plans involving interest charges.
11. Personal property and real estate appraisals.

12. Offering cards in lieu of cash for financial transactions. For example, a debit card program.
13. Planned Giving

2. What is Customer Information?

Customer information is any record containing non-public personal information about a customer whether in paper, electronic or other form, related to the covered product or service. Examples include social security number, account number, credit card numbers, date of birth, or details of any related financial transactions.
Non-public personal information means personally identifiable financial information that is:

1. Provided by a consumer to MSU;
2. Resulting from any transaction with the consumer or any service performed for the consumer; or
3. Otherwise obtained by MSU

The term non-public also includes any list, description, or other grouping of consumers and publicly available information pertaining to them that is derived using any personally identifiable financial information that is not publicly available.

3. What does "significantly engaged" mean?

The FTC regulation and final ruling provides little guidance on how to interpret "significant", but the FTC has advised that if a company holds itself out as undertaking the listed financial activities, such activities are "significant", without regard to dollar volume and without regard to the percentage of the revenue of the overall business.

Examples of entities that are not significantly engaged in financial activities.

1. A business is not a financial institution if its only means of extending credit are occasional "lay away" and deferred payment plans or accepting payment by means of credit cards issued by others.
2. A business is not a financial institution merely because it accepts payment in the form of cash, checks, or credit cards that it did not issue.
3. A business is not a financial institution merely because it allows an individual to "run a tab".
4. A business is not a financial institution merely because it allows individuals to whom it sells goods to, to cash a check, or write a check for a higher amount than the purchase and obtain cash in return.

IV. POLICY

Complying with the Safeguards Rule

1. Overview

The GLB Act covers many types of financial products and services transacted with consumers. These services include: lending, brokering or servicing any type of consumer loan; transferring or safeguarding money; preparing individual tax returns; providing financial advice or credit counseling; and an array of other activities. Such non-traditional "financial institutions" are regulated by the FTC. For more information on the types of financial activities covered, Click here.

Michigan State University collects personal information from its customers. This information may include names, addresses, and phone numbers; bank and credit card account numbers; and Social Security Numbers. The GLB Act requires that MSU, to the extent its service offerings are defined under the law as a "financial service(s)" ensure the security and confidentiality of this type of information. As part of its implementation of the GLB Act, the Federal Trade Commission (FTC) issued the Safeguards Rule, which requires MSU to have measures in place to keep customer information related to these services secure.

2. Written Plan

The Safeguards Rule requires MSU and its affected units to develop a written information security plan that describes its program(s) to protect customer information. The plan must be appropriate to MSU's size and complexity, the nature and scope of our activities and the sensitivity of the customer information it handles. As part of its plan, MSU and its affected units must:

1. designate one or more employees to coordinate its information security program (MSU Chief Information Security Officer);
2. identify and assess the risks to customer information in each relevant area of the University's operation, and evaluate the effectiveness of the current safeguards for controlling the identified risks;
3. establish an incident response plan;
4. have a qualified individual report regularly and at least annually to the Board of Trustees on the institution's information security program;
5. design and implement a safeguards program, and regularly monitor and test that program;
6. select third party vendors that can maintain appropriate safeguards, making sure that contracts with these vendors require them to maintain safeguards, and allow the University to oversee their handling of customer information; and
7. regularly evaluate and adjust the program in light of relevant circumstances, including changes in the University's business or operations, or the results of security testing and monitoring.

MSU has developed an umbrella Customer Information Security Plan for Michigan State University, as well as unit-based plans to cover their unique safeguarding requirements as dictated by their business operations. See Section VII below.

V. POLICY PROCEDURES

1. Guidelines

Some of the practices to safeguard information in place at affected units include:

1. Requesting every employee to sign an agreement to follow the University's confidentiality and security standards for handling customer information and regularly reminding them of the University's policies and legal obligations to keep customer information secure and confidential. These policies include, but are not limited to:
    1. Guidelines Governing Privacy and Release of Student Records
    2. Rules Governing Personal Conduct of Employees
    3. MSU Acceptable Use of Computing Systems, Software, and the University Digital Network
    4. Student Rights Under the Family Education Rights and Privacy Act (FERPA)
    5. Individual unit Employment Security Statement
    6. Individual unit Electronic Data Storage Policies
2. Limiting access to customer information to employees who have a business reason to see it (commonly referred to as "Need to Know").
3. Controlling access to sensitive information by requiring employees to use "strong" passwords that must be changed on a regular basis. (Strong passwords require the use of at least eight characters, upper- and lower-case letters, and a combination of letters, numbers and symbols).
4. Using password-activated screen savers to lock employee computers after a period of inactivity.
5. Maintaining up-to-date and appropriate programs and controls to prevent unauthorized access to customer information. Includes:
    1. checking with software vendors regularly to get and install patches that resolve software vulnerabilities;
    2. using anti-virus and anti-spyware software that updates automatically;
    3. maintaining up-to-date hardware firewalls;
    4. ensuring that ports not used directly for MSU business are closed; and
    5. promptly passing along information and instructions to employees regarding any new security risks or possible breaches.
6. Using appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information. Includes:
    1. keeping logs of activity on the network and monitoring them for signs of unauthorized access to customer information;
    2. using an up-to-date intrusion detection system to alert system administrators of attacks; and
    3. monitoring both in- and out-bound transfers of information for indications of a compromise.

2. Contact for Questions

Controller's Office
Hannah Administration Building
426 Auditorium Road, Room 360, East Lansing, MI 48824
Phone: (517) 355–5020

VI. VIOLATIONS

Employees or students who violate this policy may be subject to discipline.

VII. RELATED INFORMATION AND ATTACHMENTS

Customer Information Security Program for Michigan State University (umbrella plan)

Conference Report and Text of Gramm-Leach-Bliley Bill
U.S. Senate Committee on Banking, Housing, and Urban Affairs

Financial Services Modernization Act - Summary of Provisions
U.S. Senate Committee on Banking, Housing, and Urban Affairs

VIII. HISTORY

*To be completed by the Office of Audit, Risk and Compliance

Action	Description
Issued:	
Approved by:	
Revised:	