MISSISSIPPI VALLEY STATE UNIVERSITY

GLBA Information Security Plan

Overview

This Information Security Plan describes safeguards implemented by Mississippi Valley State University as mandated by the Federal Trade Commission's Safeguards Rule and the Gramm Leach Bliley Act (GLBA). This Plan is led by the Information Security Coordinator in collaboration with Directors or their designee from the respective departments including, but not limited to the Department of Information Technology ("IT") the Office of Financial Aid, and the Department of Business & Finance, Institutional Research, the Office of Admissions, and the Office of the Registrar. This program is in addition to other University policies and procedures that may be required pursuant to other federal and state laws and regulations, including Family Educational Rights and Privacy Act (FERPA).

Information Security

To comply with federal requirements to safeguard financial and other confidential information, Mississippi Valley State University (MVSU) aims to protect critical information in all forms for which it is the custodian and to maintain a proactive and evolving information security program. Information security is the responsibility of all individuals who access and maintain MVSU's information resources and each individual much be aware of and accountable for their role in the overall protection of critical information. Critical information includes any record containing non-public personal information about a student or other third party who has a continuing relationship with the University, whether in paper, electronic, or other format that is handled or maintained by or on behalf of the University. Additionally, any record containing non-public personal information pertaining to customers of other financial institutions that have provided such information to the University. For these purposes, the term non-public personal information shall mean:

- Personally identifiable financial information defined as:
    - any information a student or third party provides in order to obtain a financial product or service from the University;

- any information about a student or other third party resulting from any transaction with the University involving a financial product or service;
- any information otherwise obtained about a student or other third party in connection with providing a financial product or service to that person; or
- Any list, description or other grouping that is derived using any personally identifiable financial information that is not publicly available.

For the purpose of this policy, offering financial products and services includes offering student loans, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services. Examples of student financial information include without limitation, information a student provides to obtain a loan or other financial product or service, bank and credit card account numbers, income and credit histories and social security numbers, in both paper and electronic format. The fact that a student or third party has obtained a financial product or service from the University is also financial information.

To comply with GLBA, administrative, technical and physical safeguards will govern access, collection, distribution, processing, protection, storage, use, transmittal, disposal or other handling of information.

Gramm Leach Bliley Act Requirements

GLBA mandates that the University (i) designate an employee(s) to coordinate the Information Security Program, (ii) conduct a risk assessment of security and privacy risks, and institute a training program for all employees who have access to covered data and information.

Designation of Representative(s)

The Information Security Coordinator is responsible for working with appropriate staff persons to assess the risks associated with unauthorized transfers of covered data and information and implementing procedures to minimize those risks to the University. The Information Security Officer will accomplish these assessments through collaboration with the Gramm Leach Bliley Compliance Committee ("GLBCC"). This committee includes Directors or their designee from the respective departments, including, but not limited to the Department of Information Technology ("IT") the Office of Financial Aid, and the Department of Business & Finance, Institutional Research, the Office of Admissions, and the Office of the Registrar. Any questions regarding the implementation of the Program or the interpretation of this document should be directed to the Information Security Coordinator.

The GLBCC will work with the Information Security Coordinator to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of account information; evaluate the effectiveness of the current safeguards for controlling these risks; design and implement an administrative, technical and physical safeguards program, regularly monitor and test the program.

Risk Assessment and Safeguards

The University intends, as part of the Information Security Program, will

- Ensure the security and confidentiality of covered data and information.
- Protect against anticipated external and internal risks to the security confidentiality, and integrity of nonpublic personal information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information.

This Information Security Program also identifies mechanisms to:

- Identify and assess the risks that may threaten covered data and information maintained by MVSU;
- Develop written policies and procedures to manage and control these risks;
- Implement and review the program; and
- Adjust the program to reflect changes in technology, the sensitivity of covered data and information and internal or external threats to information security.

The University has discontinued usage of social security numbers as student identifiers. Social security numbers are considered protected information under both GLBA and the FERPA. By necessity, student social security numbers remain in the University student information system. The GLBCC will conduct an assessment to determine who has access to social security numbers, in what systems the numbers are still used, and in what instances, if any, students are inappropriately being asked to provide a social security number. This assessment will cover University employees as well as subcontractors such as student loan billing and collection services.

The Department of Information Technology will develop a plan to ensure that all electronic covered information is encrypted in transit and that the central databases are strongly protected from security risks.

The Department of Information Technology will develop plans and procedures to detect and prevent any attempted attacks, intrusions or other failures on central systems and will develop incident response procedures for actual or attempted unauthorized access to covered data or information.

The Department of Information Technology will develop and provide Departmental Lab Technicians who maintain their own servers with plans and procedures they must follow to detect attempted attacks or intrusions on central systems and incident response procedures for actual or attempted unauthorized access to covered data or information.

Administrative Safeguards

Administrative Safeguards include developing and publishing policies, standards, procedures and guidelines, and are generally within the direct control of a department, such as:

- Reference checks for potential employees.
- Confidentiality agreements that include standards for handling customer information.
- Training all MVSU employees in departments that collect, access, retain, or transmit or dispose of Covered Data on basic steps, they must take to protect customer information.
- Assure employees are knowledgeable about applicable policies and expectations.
- Limit access to customer information to employees who have a business need to see it.
- Impose disciplinary measures where appropriate.

Physical Safeguards

- Physical Safeguards are also generally within a department's control and include:
- Locking rooms and file cabinets where customer information is maintained.
- Using password activated screensavers.
- Using strong passwords.
- Changing passwords periodically and not writing them down.
- Referring calls or requests for customer information to staff trained to respond to such requests.
- Being alert to fraudulent attempts to obtain customer information and reporting these to management for referral to appropriate law enforcement agencies.
- Ensure the storage areas are protected against destructions or potential damage from physical hazards, like fire or floods.

- Store records in a secure area and limit access to authorized employees.
- Dispose of customer information appropriately.
- Shred or recycle customer information recorded on paper and store it in a secure area until the confidential recycling service picks it up.
- Erase all data when disposing of computers, diskettes, magnetic tapes, hard drives or any other electronic media that contains customer information.

Technical Safeguards

Technical Safeguards include:

- Storing electronic customer information on a secure server that is accessible only with a password or has other security protections and is kept in a physically secure area.
- Avoiding storage of customer information on machines with an Internet connection.
- Maintaining secure backup media and securing archived data.
- Using anti-virus software that updates automatically.
- Obtaining and installing patches that resolve software vulnerabilities.
- Following written contingency plans to address breaches of safeguards.
- Maintaining up-to-date firewalls particularly if the institution uses broadband Internet access or allows staff to connect to the network from home.
- Providing central management of security tools and keep employees informed of security risks and breaches.

Designing and Implementing Safeguards

The risk assessment and analysis described above shall apply to all methods of handling or disposing of non-public financial information, whether in electronic, paper or other form. The Information Security Coordinator and GLBCC will assist in implementing safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures.

This evaluation will include assessing the effectiveness of the University's current policies and procedures relating to system access, the use of the University's network, network security, documentation retention and destruction. The Information Security Coordinator will coordinate with the GLBCC and the Department of Information Technology to assess procedures for monitoring potential information security threats associated with software systems and for updating such systems, implementing patches or other software fixes designed to deal with known security flaws.

Employee Training and Management

While the directors are ultimately responsible for ensuring compliance with information security practices, the Information Security Coordinator will consult with relevant offices to provide training related to access to and use of covered information. Employees with access to covered information typically fall into three categories: professionals in information technology who have general access to all university data, Data Custodians who have access to specific systems, and those employees who use data as part of their essential job duties.

Oversight of Service Providers

The Information Security Coordinator shall consult with those responsible for the procurement of third party services and other affected departments to raise awareness of, and to institute methods for, selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for non-public personal information of students and other third parties to which they will have access. In addition, the GLBCC will work with the appropriate staff members to develop and incorporate standards, contractual protections applicable to third party service providers, which will require such providers to implement and maintain appropriate safeguards. These standards shall apply to all existing and future contracts entered into with such third party service providers.

Program Review and Revision

GLBA mandates that this Program be subject to periodic review and adjustment. The most frequent of these reviews will occur within the various policies where constantly changing technology and evolving risks indicate regular reviews. Process in the other relevant offices of the University such as data access procedures and training will undergo regular review.

This Information Security Plan will be reevaluated regularly to ensure compliance with existing and future laws and regulations.

Revision History

June, 2020; June 16, 2021

DEFINITIONS

Covered Data - (i) non-public personal financial information about a Customer and (ii) any list, description, or other grouping of Customers (and publicly available information pertaining to them) that is derived using any non-public personal financial information. Examples of Covered Data include bank and credit card account numbers, income and credit histories, tax returns and social security numbers and lists of public information such as names, addresses and telephone numbers derived in whole or in part from personally identifiable financial information (e.g., names of students with outstanding loans). Covered Data is subject to the protections of GLBA, even if the Customer ultimately is not awarded any financial aid.

Covered Data includes such information in any form, including paper and electronic records.

MVSU and **University** - Mississippi Valley State University.

Customer - any individual (student, parent, faculty, staff, or other third party with whom the University interacts) who receives a Financial Service from the University for personal, family or household reasons that results in a continuing relationship with the University.

Financial Service - includes receiving income tax information from a student or a student's parent when offering a financial aid package, engaging in debt collection activities, and leasing real or personal property to individuals for their benefit.

Service Provider - any person or entity that receives, maintains, processes, or is permitted access to Covered Data information through its direct provision of services to the University.