MERCER UNIVERSITY

Policies and Procedures Manual
Department of Information Technology

SUBJECT:	EFFECTIVE:
Information Security Program	**June 1, 2023**

This Information Security Program ("Program") describes Mercer University's safeguards to protect Covered Data and information ("Covered Data"). Covered Data for the purpose of this policy includes student financial information required to be protected under the Gramm Leach Bliley Act (GLBA). In addition to this coverage, which is required under federal law, Mercer University chooses as a matter of policy to also include in this definition any credit card information received in the course of business by the University, whether or not such credit card information is covered by GLBA. The Covered Data and information include both paper and electronic records. Student financial information is information that Mercer University has obtained from a customer in the process of offering a financial product or service, or such information provided to the University by another financial institution. Offering a financial product or service includes offering student loans to students, 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 addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.

Part 1: Introduction and Overview

1.1 Purpose

The purpose of the Program is to protect the confidentiality, integrity, and availability of Covered Data in compliance with GLBA. The Program addresses the requirements of GLBA and is designed to safeguard the Covered Data at Mercer University, considering its activities, the nature and scope of operations, and the approximately 10,000 students enrolled.

1.2 Scope

The Program applies to all employees, contractors, and third-party service providers who have access to Covered Data or are involved in the processing, storage, or transmission of Covered Data.

1.3 Objectives

The objectives of the Program are to:

a. Ensure the security and confidentiality of Covered Data.

b. Protect against any anticipated threats or hazards to the security or integrity of Covered Data.

c. Prevent unauthorized access to or use of Covered Data.

d. Detect and respond to security incidents.

e. Ensure the proper disposal of Covered Data.

Part 2: Administrative Safeguards

2.1 Risk Assessment

Mercer University recognizes that it has both internal and external risks. Mercer University's undertakes risk assessments aimed to identify reasonably foreseeable internal and external risks that could result in unauthorized disclosure, misuse, alteration, destruction, or compromise of Covered Data. The risk assessments also involve assessing the sufficiency of controls in place to mitigate identified risks.

2.1.1 Risk Identification

Mercer identifies the following as key criteria for the evaluation and categorization of identified security risks or threats:

a. Internal Risks: Employee negligence or malicious actions. Inadequate access controls and user management. Weak physical security measures. Insufficient training and awareness programs. Inadequate patch management and system updates. Poor change management practices. Inadequate incident response and business continuity plans.

b. External Risks: Cyberattacks (e.g., phishing, malware, ransomware). Data breaches targeting Covered Data. Social engineering attacks. Third-party risks (e.g., vendors, service providers). Physical security breaches (e.g., unauthorized access to facilities).

2.1.2 Assessment

Mercer University assesses the potential impact and likelihood of these risks materializing using the following criteria:

a. Confidentiality: Likelihood of unauthorized access to Covered Data. Potential impact of unauthorized disclosure or data leakage. Adequacy of encryption and access controls
b. Integrity: Likelihood of unauthorized alteration or tampering with Covered Data. Potential impact on the accuracy and reliability of Covered Data. Effectiveness of data validation and integrity checks.
c. Availability: Likelihood of service disruptions or denial of access to Covered Data. Potential impact on business operations and customer service. Sufficiency of backup and recovery mechanisms

2.1.3 Risk Mitigation or Acceptance

Based on the prioritization of identified risks, Mercer establishes the following requirements for risk mitigation:

a. Safeguard Implementation: Technical controls (e.g., firewalls, intrusion detection systems). Administrative controls (e.g., security policies, access controls). Physical controls (e.g., video surveillance, access control systems)
b. Incident Response and Business Continuity: Incident response plan for timely detection, containment, and recovery from security incidents. Business continuity plan to ensure the availability of critical systems and customer information.

c. Monitoring and Testing: Continuous monitoring of systems and network traffic for potential security incidents. Regular vulnerability assessments and penetration testing. Ongoing security awareness training for employees.

d. Third-Party Management: Due diligence in selecting and monitoring third-party vendors. Contractual agreements to ensure they adhere to security requirements.

e. Risk Acceptance: In cases where the cost of mitigation outweighs the potential impact, risks may be accepted after senior management approval. Adequate documentation and justification for risk acceptance decisions.

2.1.4 Ongoing Assessment

Mercer University recognizes that this may not be a complete list of the risks associated with the protection of Covered Data and information. Since technology growth is not static, new risks are created regularly. Accordingly, the Information Technology team will actively participate and monitor advisory groups for identification of new risks. Mercer University believes Information Technology's current safeguards are reasonable and, in light of Information Technology's current risk assessments are sufficient to provide security and confidentiality to Covered Data and information maintained by the University. Additionally, these safeguards protect against current known threats or hazards to the integrity of such information.

2.2 Qualified Individual

Mercer University has appointed an internal qualified individual to be responsible for overseeing the Program. This person has the necessary knowledge, skills, and experience in information security to be responsible for implementing and managing the Program, conducting regular risk assessments, and ensuring compliance with GLBA requirements. This person also stays updated on emerging threats and best practices to continually enhance the effectiveness of the program. Additionally, the appointed qualified individual shall work with the other employees of Mercer for development, deployment, and execution of associated plans and policies indicated within the Program.

2.3 Employee Training and Awareness

Mercer University recognizes that employees play a critical role in maintaining the security of Covered Data. Therefore, the university shall implement a comprehensive Security Education and Training Awareness (SETA) program for employees that regularly work with Covered Data and information that includes the following components:

a. Background Checks: References of new employees will be checked.
b. General Security Awareness Training: All employees, contractors, and third-party service providers shall receive regular security awareness training to educate them about the importance of information security, common threats and vulnerabilities, and their responsibilities in safeguarding Covered Data. The training will cover topics such as password hygiene, phishing awareness, social engineering, and best practices for secure data handling.

c. Role-Based Training: Different roles within the organization may have specific security responsibilities. Role-based training will be provided to employees based on their job functions and the level of access they have to Covered Data. This training will focus on the specific security controls, procedures, and policies relevant to their roles.
d. Incident Response Training: Employees shall receive training on how to recognize and respond to security incidents. This training will include reporting procedures, incident escalation processes, and their roles and responsibilities during incident response. Employees will be educated on the importance of prompt reporting to minimize the impact of security incidents.
e. Policy and Procedure Training: All employees shall be trained on the organization's information security policies and procedures. This training will ensure that employees understand their obligations, follow the prescribed security practices, and are aware of the consequences of non-compliance.
f. Ongoing Training and Awareness: Mercer University will promote a culture of security awareness by providing ongoing training and awareness campaigns to reinforce best practices, new threats, and emerging trends in information security. This may include regular security updates, newsletters, and periodic refresher training sessions.

The employee training program shall be regularly evaluated for its effectiveness, and training records will be maintained to ensure compliance and track the completion of training activities by employees. By implementing these additional measures, Mercer University aims to enhance the security of Covered Data, strengthen its defenses

against cyber threats, and ensure that employees have the knowledge and skills to support a secure information environment.

2.4 Written Policies and Procedures

Mercer University develops and maintains written information security policies and procedures that address the protection of customer information. These policies and procedures are reviewed and updated periodically to reflect changes in technology, threats, and business operations.

2.5 Incident Response Plan

Mercer has developed, documented, and implemented an incident response plan to ensure timely and effective response to security incidents. The plan includes procedures for reporting, assessing, containing, mitigating, and recovering from security incidents.

Part 3: Technical Safeguards

3.1 Access Control

Mercer University implements access controls to ensure that only authorized individuals have access to customer information. This includes strong authentication mechanisms, user access reviews, and least privilege principles. Additionally, Multi-Factor Authentication (MFA) shall be required for all systems and applications that store or process Covered Data. This additional layer of security will help prevent unauthorized access even if passwords are compromised.

3.2 Encryption

Covered Data transmitted over public networks or stored on portable devices shall be encrypted using industry-standard encryption algorithms and protocols. Mercer University will ensure that all Covered Data is encrypted both at rest and in transit. Encryption at rest refers to the encryption of data when stored on servers, databases, or other storage devices. Encryption in transit refers to the encryption of data during transmission over networks or between systems.

3.3 System and Network Security

Mercer University implements appropriate security measures to protect its systems and networks from unauthorized access, including firewalls, intrusion detection systems, and regular vulnerability assessments.

3.4 Malware Protection

Up-to-date anti-malware software shall be deployed on all systems to detect and prevent the execution of malicious code, including viruses, worms, and ransomware.

3.5 Data Backup and Recovery

Regular data backups shall be performed to ensure the availability and integrity of Covered Data. Backup data shall be stored securely onsite and offsite. Backups shall be tested periodically for recoverability.

3.6 Annual Penetration Testing

To ensure the effectiveness of security controls, Mercer University shall contract annual penetration testing of its systems and networks. Penetration testing will involve authorized simulated attacks to identify vulnerabilities and weaknesses that could be exploited by malicious actors. The testing shall be performed by qualified and independent third-party assessors who assess the university's infrastructure, applications, and configurations. The results of the testing will be used to remediate any identified vulnerabilities and strengthen the overall security posture.

3.7 Vendor Auditing

Due to the specialized expertise needed to design, implement, and service new technologies, vendors may be needed to provide resources that Mercer University determines not to provide on its own. Mercer University recognizes the importance of assessing the security practices of its third-party vendors and service providers which have access to Mercer’s Covered Data. The university uses a vendor management program that includes periodic audits and assessments of vendors' information security controls. Vendors are required to complete annual questionnaires that evaluate their security measures, including data handling practices, access controls, incident response procedures, and compliance with applicable regulations. The questionnaire responses are reviewed and assessed to ensure that vendors meet the

required security standards. Contracts with service providers may include the following provisions:

a. An explicit acknowledgement that the contract allows the contract partner access to Covered Data.
b. A specific definition or description of the Covered Data being provided.
c. A stipulation that the Covered Data will be held in strict confidence and accessed only for the explicit business purpose of the contract.
d. An assurance from the contract partner that the partner will protect the Covered Data it receives according to commercially acceptable standards and no less rigorously than it protects its own confidential information.
e. A provision providing for the return or destruction of all Covered Data received by the contract provider upon completion or termination of the contract.
f. An agreement that any violation of the contract's confidentiality conditions may constitute a material breach of the contract and entitles Mercer University to terminate the contract without penalty.
g. A provision ensuring that the contract's confidentiality requirements shall survive any termination agreement.

Part 4: Physical Safeguards

4.1 Facility Security

Access to facilities where Covered Data is stored or processed shall be restricted to authorized personnel only. Physical access controls, such as locks, badges, and surveillance systems, shall be implemented to protect against unauthorized entry.

4.2 Secure Disposal of Covered Data

Procedures shall be established to ensure the proper disposal of customer information in a secure manner. This includes shredding or secure wiping of physical documents and secure erasure of electronic media.

4.3 Incident Monitoring and Reporting

Mercer University implements systems and processes to monitor security incidents, including unauthorized access attempts, malware infections, and other indicators of compromise. Incidents shall be reported, documented, and appropriate actions taken to mitigate and prevent future occurrences.

Part 5: Program Review and Update

5.1 Program Review

By implementing this comprehensive Program, Mercer University aims to protect customer information, prevent security breaches, and maintain compliance with GLBA requirements. The Program shall be reviewed periodically to assess its effectiveness, address any identified deficiencies, and ensure ongoing compliance with GLBA requirements. The review shall include an evaluation of security controls, incident response effectiveness, and any changes in the operating environment.

5.2 Program Update

The Program shall be updated as necessary to reflect changes in technology, threats, regulatory requirements, and business operations. Updates may include revisions to policies and procedures, security controls, training programs, and incident response plans.