GLBA Information Security Program

As it pertains to the Gramm Leach Bliley Act, Safeguarding of Electronic Customer Information for the Gramm Leach Bliley Act (GLBA):

- Ensure the security and confidentiality of customer information in compliance with applicable GLBA rules as published by the Federal Trade Commission.
- Safeguard against anticipated threats to the security or integrity of protected electronic data.
- Guard against unauthorized access to or use of protected data that could result in harm or inconvenience to any customer.

Information Security Program

As it pertains to the Gramm Leach Bliley Act, Safeguarding of Electronic Customer Information for the Gramm Leach Bliley Act (GLBA):

- Ensure the security and confidentiality of customer information in compliance with applicable GLBA rules as published by the Federal Trade Commission.
- Safeguard against anticipated threats to the security or integrity of protected electronic data.
- Guard against unauthorized access to or use of protected data that could result in harm or inconvenience to any customer.

Contents

I. Coordination and Responsibility for the Information Security Program

The Coordinator of the Information Security Program is the Coordinator for Campus Services & Solutions for Greenville University. The Coordinator is responsible for the development, implementation, and oversight of Greenville University's compliance with the policies and procedures required by the Gramm Leach Bliley Act (GLBA) Safeguards Rule. Although ultimate responsibility for compliance lies with the Coordinator, representatives from each of the operational areas are responsible for implementation and maintenance of the specified requirements of the security program in their specific operation.

See Appendix A for the matrix identifying the GLBA operational areas and their representatives. Appendix B includes a list of areas considered for inclusion in this program, but deemed to be outside the scope of the GLBA Safeguards Rule.

Information Security Governance Committee
The above referenced Committee exists to ensure that this Information Security Program is kept current and to evaluate potential policy or procedural changes driven by GLBA. Committee membership may change from time-to-time but will minimally include the Coordinator for Campus Services & Solutions, Controller, Director of Financial Aid, and Assistant Director of Financial Aid & Compliance Officer. Other individuals may be added as deemed necessary.

Questions regarding GLBA impacts on business processes and policies should be directed to the Coordinator of the Information Security Program, and questions regarding technical issues, risk assessments, and information technology security policy should be directed to the Office of Information Technology Data Security and Privacy Policy.

II. Risk Assessment and Safeguards

There is an inherent risk in handling and storing any information that must be protected. Identifying areas of risk and maintaining appropriate safeguards can reduce risk. Safeguards are designed to reduce the risk inherent in handling protected information and include safeguards for information systems and the storage of paper.

III. Employee Training and Education

Employees handle and have access to protected information in order to perform their job duties. This includes permanent and temporary employees as well as student employees, whose job duties require them to access protected information or who work in a location where there is access to protected information. Departments are responsible for maintaining a high level of awareness and sensitivity to safeguarding protected information and should periodically remind employees of its importance. Seemingly minor changes to office layout and practices could significantly compromise protected information if a culture of awareness is not present.

The department representative is responsible for ensuring that staff members are trained in the relevant GLBA concepts and requirements.

IV. Oversight of Service Providers and Contracts

GLBA requires the University to take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. The Office of Legal Counsel has assisted with language to ensure that all relevant service provider contracts comply with GLBA provisions. Contracts should be reviewed to ensure the following language is included:

[Service Provider] agrees to implement and maintain a written comprehensive information security program containing administrative, technical and physical safeguards for the security and protection of customer information and further containing each of the elements set forth in § 314.4 of the Gramm Leach Bliley Standards for Safeguarding Customer Information (16 C.F.R. § 314). [Service Provider] further agrees to safeguard all customer information provided to it under this Agreement in accordance with its information security program and the Standards for Safeguarding Customer Information.

The GLBA contract due diligence is considered in various aspects of contract negotiation, including security control reviews.

V. Evaluation and Revision of the Information Security Program

GLBA mandates that this Information Security Program be subject to periodic review and adjustment. The most frequent of these reviews will occur within the Data Security and Privacy Policy where constantly changing technology and constantly evolving risks indicate the wisdom of regular reviews. Processes in other relevant offices of the University such as data access procedures and the training programs should undergo regular review.

This Information Security Program is reevaluated regularly in order to ensure ongoing compliance with existing and future laws and regulations.