Bryant University
GRAMM LEACH BLILEY ACT Plan

I. OVERVIEW

A. Purpose
In order to continue to protect critical information and data, and to comply with Federal law, Bryant University (the University) adopts this Information Security Program (the Program) in accordance with the Safeguards Rule issued by the Federal Trade Commission. As required by the Safeguards Rule, and to the extent that the University is classified as a financial institution under the GLBA, this Program is designed to provide for the security and confidentiality of nonpublic customer personal information ("covered data"), protect against anticipated threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to a customer. The GLBA also requires financial institutions to comply with its privacy regulations; however, the University is in compliance by virtue of the privacy provisions in the Family Educational Rights and Privacy Act (FERPA).

B. Scope of Program – Definitions
Nonpublic customer personal information means any personally identifiable information, not otherwise publicly available, that the University has obtained from a student, student's parent or spouse, employee, alumnus, or other third party, in the process of offering a financial product or service, OR such information provided to the University by another financial institution, OR such information otherwise obtained by the University in connection with providing a financial product or service. *Offering a financial product or service* includes such activities as student loans, and other miscellaneous financial services as defined in regulations contained in 12 CFR Section 225.28 of the Federal Trade Commission. Examples of personally identifiable financial information include social security numbers, bank account numbers, account balances, credit card numbers, income and credit histories or ratings, and tax returns, and asset statements, in both paper and electronic form. *Publicly available* for purposes of this Plan means information that the University has a reasonable basis to believe is lawfully available to the general public from government records, widely distributed media, or disclosures to the general public required under law. Examples of publicly available financial information include, but are not limited to, listings in telephone and online directories and financial information contained in recorded deeds of trust, judgments, or liens. *Covered data* and information includes nonpublic customer personal information requiring protection under the GLBA.

II. PROGRAM COMPONENTS

This Information Security Program has five components:
(1) Designating a program coordinator;
(2) Conducting risk assessments to identify reasonably foreseeable security and privacy risks;

(3) Ensuring that safeguards are employed to control the risks identified and that the effectiveness of these safeguards is regularly tested and monitored;
(4) Overseeing service providers; and
(5) Maintaining and adjusting this Information Security Program based upon results of testing and monitoring conducted as well as changes in operations or operating systems.

A. Program Coordination: Designation of Representatives

The Information Security Program Committee (ISPC) is responsible for coordinating and overseeing the Program. The ISPC consists of administrators from various departments across the University. The Committee may designate other representatives of the University to oversee and coordinate particular elements of the Program. Any questions regarding the implementation of the Program or the interpretation of this document should be directed to the chair of the ISPC.

The Committee is responsible to assure that, based on the University's risk assessments, safeguards are employed to control the risks identified. The Committee will act as a consultant to and will work with responsible parties ("Data Custodians") that have access to or maintain information that is covered by GLBA to ensure adequate training and education is developed and delivered. The Committee will, on a regular basis, assist Data Custodians in the testing and monitoring of safeguards, and work with responsible parties to verify that existing policies, standards and guidelines are reviewed and adequate for the security of covered data. The Committee will make recommendations for revisions to this Program, University policy, or the development of new policy, as appropriate. The Committee will conduct an annual review and provide an update on the status of the GLBA Plan.

B. Risk Assessment

Offices or departments handling covered data and information as identified by the Committee will identify and assess internal and external risks to the security, confidentiality, and integrity of covered data and information that could result in the unauthorized access, disclosure, misuse, alteration, destruction or other compromise of such information. Each Data Custodian should conduct an annual risk assessment, with guidance from the Committee. This risk assessment will include, but not be limited to, consideration of risks, and current safeguards to manage those risks, to covered data and information in each relevant aspect of University operations, including: employee, student worker, and volunteer training and management regarding access to and use of such information; information systems (including network and software design, as well as information processing, storage, transmission and disposal of both electronic and paper records); and detecting, preventing, and responding to attacks, intrusions, or other system failures (including data processing and telephone communication), as well as contingency planning and business continuity. The Committee may identify a responsible party from offices or departments handling covered data and information to periodically identify risks to the security, confidentiality and integrity of covered data within the affected office or department.

C. Design, Implementation, and Monitoring of Safeguards

Each affected office or department will design, implement, and maintain in writing such administrative, technical, and physical safeguards as are necessary to control the risks identified through risk assessment, and will regularly monitor the effectiveness of such safeguards. The Committee will draft and implement safeguards, and provide training regarding those safeguards, as necessary.

1. Employee Training and Management

Individuals with authorized access to covered data will receive training and education regarding University policies, standards and guidelines for preserving the security of confidential information, including covered data. Other safeguards will also be used, as appropriate, including: job-specific training on maintaining security and confidentiality; requiring user-specific passwords and periodic changes to those passwords; limiting access to covered data to those with a business need for access to information; requiring signed certification of responsibilities prior to authorizing access to systems with covered data; requiring signed releases for disclosure of covered data; establishing methods for prompt reporting of loss or theft of covered data or media upon which covered data may be stored; and other measures that provide reasonable safeguards based upon the risks identified.

2. Information Systems

Information systems include network and software design, as well as information processing, storage, transmission, retrieval, and disposal. The University will maintain effective systems to prevent, detect, and respond to attacks, intrusions and other system failures.

D. Oversight of Service Providers and Contract Assurances

The GLBA requires the University to take reasonable steps to select and retain services providers who maintain appropriate safeguards for covered data and information. A "Service provider" is any person or entity that receives, maintains, processes, or otherwise is permitted to access covered data and information through its provision of services directly to processes, or otherwise is permitted to access covered data and information through its provision of services directly to the University. GLBA certification is required of each Service provider and will be retained as part of the University's GLBA plan.

E. Evaluation and Revision of the Information Security Program

The GLBA mandates that this Plan be subject to periodic review and adjustments to ensure compliance with laws and regulations. The most frequent of these reviews will likely occur with the office of Information Services where operations involve constantly changing technology and evolving risks. Processes in other relevant offices of the University should also be reviewed regularly, particularly as appropriate to any operational changes that may have a material impact on the Plan. The Committee will review the Plan annually to assure ongoing compliance with the GLBA and the Federal Trade Commission Safeguards Rule, as well as consistency with other existing and future laws and regulations.