Customer Information Security Program and GLBA Policy

Overview

The Gramm-Leach-Bliley Act, (GLBA) effective May 23, 2003, addresses the safeguarding and confidentiality of customer information held in the possession of financial institutions such as banks and investment companies. GLBA contains no exemption for colleges or universities. As a result, educational entities that engage in financial activities, such as processing student loans, are required to comply. GLBA and other emerging legislation could result in standards of care for information security across all areas of data management practices both electronic and physical (employee, student, customer, alumni, donor, etc.). Therefore, Coyne College has adopted a Customer Information Security Program for certain highly critical and private financial and related information. This security program applies to customer financial information (covered data) the College receives in the course of business as required by GLBA as well as other confidential financial information the College has voluntarily chosen as a matter of policy to include within its scope.

This document describes many of the activities the College currently undertakes, and will undertake, to maintain covered data according to legal and College requirements. This Information Security Program document is designed to provide an outline of the safeguards that apply to this information, specifically in compliance with GLBA. The practices set forth in this document will be carried out by and impact diverse areas of the College.

Definitions

Customer - means any individual who receives a financial service from the College. Customers may include students, parents, spouses, faculty, staff, and third parties.

Non-public personal information - means any personally identifiable financial or other personal information, not otherwise publicly available, that the College has obtained from a customer in the process of offering a financial product or service; such information provided to the College by another financial institution; such information otherwise obtained by the College in connection with providing a financial product or service; or any list, description, or other grouping of customers (and publicly available information pertaining to them) that is derived using any information listed above that is not publicly available. Examples of personally identifiable financial information include names, addresses, telephone numbers, bank and credit card account numbers, income and credit histories, tax returns, asset statements, and social security numbers, both in paper and electronic form.

Financial product or service - includes student loans, employee loans, activities related to extending credit, financial and investment advisory activities, management consulting and

counseling activities, community development activities, and other miscellaneous financial services as defined in 12 CFR § 225.28.

Covered data and information - for the purpose of this Program includes non-public personal information of customers required to be protected under GLBA. In addition to this required coverage, the College chooses as a matter of policy to also define covered data and information to include any bank and credit card account numbers, income and credit information, tax returns, asset statements, and social security numbers received in the course of business by the College, whether or not such financial information is covered by GLBA. Covered data and information includes both paper and electronic records.

Security Program Components

The GLBA requires that the College develop, implement, and maintain a comprehensive information security program containing the administrative, technical, and physical safeguards that are appropriate based upon the College's size, complexity, and the nature of its activities. This Information Security Program has five components:

1. designating an employee or office responsible for coordinating the program;
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;
5. maintaining and adjusting this Information Security Program based upon the results of testing and monitoring conducted as well as changes in operations or operating systems.

Security Program Coordinator

The GLBA Security Program Coordinator (Coordinator) will be responsible for implementing this Information Security Program. The Coordinator shall be appointed by the School Director. The Coordinator will work closely with the President, Director, Registrar, Bursar, Student Accounts, and Financial Aid, and such other offices and units as may have interface with or control over covered data.

The Coordinator will consult with responsible offices to identify units and areas of the College with access to covered data. As part of this Information Security Program, the Coordinator has identified units and areas of the College with access to covered data. The Coordinator will conduct a survey, or utilize other reasonable measures, to confirm that all areas with covered information are included within the scope of this Information Security Program. The Coordinator will maintain a list of areas and units of the College with access to covered data.

The Coordinator will ensure that risk assessments and monitoring are carried out for each unit or area that has covered data and that appropriate controls are in place for the identified risks.

The Coordinator will work with responsible parties to ensure adequate training and education is developed and delivered for all employees with access to covered data. The Coordinator will, in consultation with other College offices, verify that existing policies, standards and guidelines that provide for the security of covered data are reviewed and adequate. The Coordinator will make recommendations for revisions to policy, or the development of new policy, as appropriate.

The Coordinator will update this Information Security Program, including this and related documents, from time to time. The Coordinator will maintain a written security plan and make the plan available to the College community.

Risk Assessment

The Information Security Program will identify reasonably foreseeable external and internal risks to the security, confidentiality, and integrity of covered data that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information and assess the sufficiency of any safeguards in place to control these risks.

The Coordinator will work with all relevant areas to carry out comprehensive risk assessments. Risk assessments will include system-wide risks as well as risks unique to each area with covered data.

Information Safeguards and Monitoring

The Information Security Program will verify that information safeguards are designed and implemented to control the risks identified in the risk assessments set forth above. The Coordinator will ensure that reasonable safeguards and monitoring are implemented and cover each unit that has access to covered data. Such safeguards and monitoring will include the following:

A. Employee Management and Training - Safeguards for security will include management and training of those individuals with authorized access to covered data. The College has adopted (or will adopt) comprehensive policies, standards and guidelines setting forth the procedures and recommendations for preserving the security of private information, including covered data.

The Coordinator will, working with other responsible offices and units, identify categories of employees or others who have access to covered data.

B. Information Systems - Information systems include network and software design, as well as information processing, storage, transmission, retrieval, and disposal.

Network and software systems will be reasonably designed to limit the risk of unauthorized access to covered data. This may include designing limitations to access, and maintaining

appropriate screening programs to detect computer hackers and viruses and implementing security patches.

C. Managing System Failures - The College will maintain effective systems to prevent, detect, and respond to attacks, intrusions and other system failures.

D. Monitoring and Testing - Monitoring systems will be implemented to regularly test and monitor the effectiveness of information security safeguards.

Service Providers

In the course of business, the College may from time to time appropriately share covered data with third parties. Such activities may include collection activities, transmission of documents, transfer of funds, destruction of documents or equipment, or other similar services. This Information Security Program will ensure that reasonable steps are taken to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue and requiring service providers by contract to implement and maintain such safeguards.

The Coordinator, by survey or other reasonable means, will identify service providers who are provided access to covered data. The Coordinator will work with other offices as appropriate to make certain that service provider contracts contain appropriate terms to protect the security of covered data.

Program Maintenance

The Coordinator, working with responsible units and offices, will evaluate and adjust the Information Security Program in light of the results of testing and monitoring described above, as well as in response to any material changes to operations or business arrangements and any other circumstances which may reasonably have an impact on the Information Security Program.

Roles and Responsibilities

Managers – Managers responsible for managing employees with access to covered data will designate a responsible contact to work with the Coordinator to assist in implementing this program. The designated contact will ensure that risk assessments are carried out for that unit and that monitoring based upon those risks takes place. The designated responsible contact will report the status of the Information Security Program for covered data accessible in that unit to the Coordinator

Employees with Access to Covered Data – Employees with access to covered data must abide by College policies and procedures governing covered data as well as any additional practices or procedures established by their unit heads or directors.

11.0 Related Policies, Standards, Guidelines

The College has adopted comprehensive policies, standards, and guidelines relating to information security. This Information Security Program incorporates by reference the College's policies and procedures in addition to any institutional policies and procedures that may be required pursuant to other federal and state laws and regulations.

Information on related information security policy and on other compliance areas at UGA can be found at the Office of Information Security Policies and Regulations page.