

# Connecticut State University System Office Information Security Policy

## I. Purpose

The Gramm-Leach-Bliley Act, [15 U.S.C. § 6801](#), et seq. (the “GLB Act”) requires that financial institutions, including colleges and universities, develop, implement and maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards appropriate to the size and complexity of the institution, the nature and scope of its activities, and the sensitivity of the customer information or data at issue. The Connecticut State University System Office (the “System Office”) has adopted this Information Security Program in order to comply with the GLB Act and the rules and regulations promulgated thereunder, to continue to ensure the security and confidentiality of customer information and data, to protect against anticipated threats or hazards to the security and confidentiality of such information, and to protect such information against unauthorized access or use which could result in substantial harm to a customer. This Information Security Program applies to customer financial information (“covered data and information”) that the System Office receives in the course of business as required by federal law, as well as to other information that the System Office has voluntarily chosen as a matter of policy to include within its scope.

## II. Definitions

**“Covered data and information”** means all customer data and information required to be protected under GLB, whether in paper, electronic or other form. “Covered data and information” also refers to financial information that the System Office has obtained from a customer in the process of offering a financial product or service, or such information provided to the System Office by another financial institution. “Offering a financial product or service” to a customer includes offering student loans, receiving income tax information from a current or prospective student or that student’s parent(s) or legal guardian(s) as part of a financial aid application, offering credit or interest bearing loans, and other miscellaneous financial services as defined in 12 C.F.R. §225.28. Examples of “covered data and information” relating to such products or services are names, addresses, phone numbers, bank and credit card account numbers, income and credit histories and social security numbers. “Covered data and information” shall also include any credit card information received in the course of business by the System Office, whether or not such credit card information is covered by GLB.

**“Service provider”** means any person or entity that receives, maintains, processes, or otherwise is permitted access to covered data and information through its provision of services to the System Office. Service providers may include, for example, businesses retained to transport, store and/or dispose of covered data and information, collection agencies, and system support providers.

### **III. Security Program Components**

This Information Security Program has five components:

- (i) Designation of departments and employees within those departments, responsible for coordinating the program;
- (ii) Implementation of risk assessment procedures to identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of customer information;
- (iii) Design and implementation of information safeguards to control the risks identified, monitoring of the effectiveness of the safeguards' key controls, systems and procedures, and updating the safeguards as necessary;
- (iv) Overseeing of service providers; and
- (v) Evaluation and adjustment of the program in response to the results of the monitoring conducted pursuant to the program as well as changes in operations or operating systems.

### **IV. Security Program Coordinators**

The System Office will designate two Security Program Coordinators, the Functional Coordinator and the Information Technology ("IT") Coordinator (together the "Coordinators"). The Executive Officer for Finance is designated the Functional Coordinator and the Executive Officer for IT is designated the IT Coordinator. The Functional Coordinator will be primarily responsible for the development and implementation of information security policies and procedures of general application throughout the System Office. The IT Coordinator will be primarily responsible for the development of policies and procedures relating to security in the area of information technology. The Coordinators together will be responsible for implementing this Information Security Program and will work with System Office personnel and the Assistant Attorney General assigned to the System Office to implement the program.

The Coordinators will consult with appropriate System Office personnel to identify departments within the System Office with access to covered data and information and shall maintain a list of such departments. For each such department, the Coordinators will ensure that the risk assessments and monitoring, addressed in sections V and VI hereof, are performed and that appropriate safeguards are instituted to control the risks identified.

The Coordinators, in conjunction with appropriate System Office personnel, will ensure that adequate training and education is provided to all System Office employees with access to covered data and information.

## **V. Risk Assessment**

The Coordinators, in conjunction with appropriate System Office personnel, will identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of covered data and information and evaluate the effectiveness of the safeguards currently in place for controlling these risks. The Coordinators, in conjunction with appropriate System Office personnel, will conduct risk assessments which shall include, but not be limited to: an assessment of employee training and management; a review of information systems utilized, including network and software design, and information processing, storage, transmission and disposal systems; and a review of the System's procedures for detecting, preventing and responding to attacks, intrusions and system failures.

Risk assessments will include System-wide risks, as well as those unique to each department having access to Covered Data and Information. Risk assessments will be conducted at least biennially, and more frequently as required.

## **VI. Design and Implementation of Information Safeguards**

A. Information Safeguards: The Coordinators, in conjunction with appropriate System Office personnel, will develop and implement information safeguards designed to control the risks to the security, confidentiality and integrity of covered data and information identified as a result of the risk assessment performed pursuant to section V hereof. The information safeguards that have been implemented by the System Office include, at a minimum:

- (i) Ensuring that only System Office staff with a business necessity have access to covered data and information;
- (ii) Ensuring the physical security of each location at which customer information is stored, whether in paper or electronic form;
- (iii) Encryption of electronic data in transit with SSL;
- (iv) Adherence to existing change management processes for customer information system modifications;
- (v) Adherence to existing dual control procedures for the granting of access to covered data and information, and continued segregation of employee duties as applicable;
- (vi) Utilization and continual monitoring of systems and procedures, including firewall and filtering technology and intrusion detection programs, which detect any actual or attempted attacks or intrusion on information systems;
- (vii) Implementing and maintaining current anti-virus software;

- (viii) Consulting with software vendors and others to regularly obtain and install patches to correct software vulnerabilities;
- (ix) Adherence to the existing program for responding to attempted and actual unauthorized access to covered data and information, including maintenance of a log of each such incident and the action(s) taken in response thereto;
- (x) Maintenance of a disaster recovery program for all servers which contain covered data and information, which program includes the daily backup of electronic information and the storage of tapes at a secure off-site facility;
- (xi) Alerting those with access to covered data and information of threats to security; and
- (xii) Use of multiple passwords that are changed periodically.

B. Testing and Monitoring: The Coordinators will take appropriate steps to ensure that monitoring systems are implemented to regularly test and monitor the effectiveness of the information safeguards' key controls, systems and procedures, and that those controls, systems and procedures are updated as necessary. The monitoring performed will include regular review of logs, employment of various system checks and restrictions, reporting of access to systems, and other reasonable measures adequate to ensure that the controls, systems and procedures are functioning properly.

C. Managing System Failures: The Coordinators will take appropriate steps to ensure that the System Office implements and maintains effective systems to prevent, detect and respond to attacks and intrusions upon the system, as well as system failures. The systems which the System Office currently employs and will continue to employ include utilizing current anti-virus and intrusion detection software, regularly obtaining and installing patches to address software vulnerabilities, utilizing appropriate filtering and/or firewall technologies, backing up data regularly and storing backed-up data off site, alerting employees with access to covered data and information of system failures, installing and maintaining uninterruptible power supplies, installing and maintaining water and heat detection devices, and installing and maintaining fire suppression and sprinkler systems. System Office will implement other reasonable measures to protect the integrity and security of its information systems as appropriate.

D. Employee Training and Management: The Coordinators will, in conjunction with appropriate System Office personnel, identify categories of employees with access to covered data and information. The Coordinators will ensure that appropriate information security training is provided to all new and existing employees who have or will have access to Covered Data and Information. The training provided will cover relevant System Office policies and procedures relating to access to Covered Data and Information, and, as appropriate, the safeguards in place or developed to protect such data and information. In connection with such training, new and existing employees will

be provided copies of those System Office policies and procedures relating to information security which are relevant to their positions, and will be required to sign an acknowledgment stating that they have read, understand, and agree to abide by those policies and procedures. The Coordinators will ensure that updated versions of System Office policies and procedures relating to information security are distributed to employees with access to Covered Data and Information, as necessary. In addition, all System Office employees will be reminded periodically (but no less frequently than annually) of the importance of adhering to the System's policies and procedures.

## **VII. Program Evaluation and Adjustment**

The Coordinators, working with appropriate System Office personnel, will evaluate the effectiveness of the Information Security Program in light of the results of the testing and monitoring described in Section VI hereof, as well as any material changes in business operations or arrangements and any other circumstance which may have a material effect on the System's Information Security Program, and will ensure that any adjustments to the Program necessary to ensure the continued security of Covered Data and Information are identified and implemented.

## **VIII. Service Providers**

In the course of its business, the System Office may appropriately share covered data and information with third parties from which it receives a service. The services provided by these third parties may include, for example, debt collection, the transmission, storage and/or destruction of documents, and the servicing of the System's information technology system.

The Coordinators will identify service providers that are currently provided access to covered data and information. The Coordinators will work with the Assistant Attorney General and other appropriate System Office personnel to ensure that existing contracts with such service providers are amended to contain appropriate terms to protect the security and confidentiality of covered data and information. The Coordinators will work with the Assistant Attorney General and other appropriate System Office personnel to develop such contract terms to be inserted into future contracts with service providers to which or access to covered data and information will be afforded. In addition, each service provider that is or will be provided access to covered data and information will be requested to provide a copy of its information security policy to the System Office for review.

## **IX. Continuing Evaluation and Adjustment**

This Information Security Policy will be subject to periodic review and revision, as circumstances, including, but not limited to, changes in technology and threats to the security of covered data and information, require.

**X. Policies, Standards and Guidelines**

The System Office has developed various policies, standards and guidelines relating to the security of its information systems. Those policies, standards and guidelines, which are hereby incorporated by reference into this Information Security Policy, include the CSU System Office Policy on Administrative Access to Electronic Data and the CSU System Office Remote Access Policy.