The City University of New York
Gramm-Leach-Bliley Information Security Program

OVERVIEW

The City University of New York (CUNY) is committed to the ongoing protection of confidential financial information. The Federal Trade Commission has issued the Safeguards Rule under the Gramm-Leach-Bliley (GLB) Act, requiring CUNY to develop, implement and maintain a comprehensive information security program to ensure the privacy of certain categories of confidential financial information. For the purpose of CUNY's Information Security Program, "Confidential Financial Information" means all nonpublic personal information, whether in paper, electronic or other form, that CUNY obtains in connection with transactions involving financial products or services offered by CUNY, such as Perkins Loans and other loans given by CUNY to students. This Information Security Program establishes CUNY's policy for the ongoing protection of Confidential Financial Information and serves as written evidence of an information security program in compliance with 16 CFR 314.3(a).

What are the objectives of the GLB Safeguards Rule and required elements of an information security program?

The objectives of the GLB Safeguards Rule are to:

- Protect the security and confidentiality of nonpublic personal information about a customer of a financial institution;
- 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 any customer.

The required elements of an information security program are to:

- Designate one or more employees to coordinate the program;
- Identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards currently in place to control these risks;
- Design and implement safeguards to control the identified risks and regularly test and monitor the effectiveness of these safeguards;
- Oversee service providers by retaining providers who are capable of maintaining appropriate safeguards and requiring the providers by contract to implement and maintain such safeguards; and
- Periodically evaluate and adjust the information security program in light of the results of the required testing and monitoring and any other circumstances that may have a material impact on the information security program.

CUNY's Information Security Program addresses the elements required by the GLB Safeguards Rule.

I. Designation of Program Coordinators

The University Central Office will designate a University Program Coordinator, who will administer CUNY's Information Security Program for the Central Office and also serve as the primary University resource and liaison with the Colleges for addressing issues related to the GLB Safeguards Rule and disseminating relevant information and updates.

In addition, the President of each College will designate a College Program Coordinator for his or her campus. Suggested College Program Coordinators include the Information Security Officer, the Record Retention Officer and the Legal Affairs Designee at the College. The Internal Control Officer at the College should not be designated the College Program Coordinator in order to avoid any potential conflict of interest.

Each College Program Coordinator should work in cooperation with the following departments and individuals: the College's Office of Legal Affairs and/or the University's Office of the General Counsel, the College's Internal Control Officer, the University Office of Internal Audit and Management Services, the University Program Coordinator, and any department in the College and the University Central Office that collects, accesses, retains, transmits or disposes of information related to any programs or processes that the University identifies as covered by the GLB Safeguards Rule (e.g., Perkins Student Loan processes).

The College Program Coordinator should also work with the College's Office of Legal Affairs and/or the University's Office of the General Counsel, the College's Business Office/Purchasing Department, the University Contracting Office, the University's Office of Computer and Information Services, and other relevant departments to identify third-party service providers who may have access to this Confidential Financial Information so that the University secures contracts with these service providers that will ensure the protection of the Confidential Financial Information.

II. Identification of Risks and Risk Assessment

CUNY recognizes that there are both internal and external risks associated with the protection of Confidential Financial Information. These risks include but are not limited to:

- Unauthorized access to Confidential Financial Information;
- Compromised system security as a result of system access by an unauthorized person;
- Interception of data during transmission;
- Loss of data integrity;
- Physical loss of data in a disaster;
- Errors introduced into the system;
- Corruption of data or systems;
- Unauthorized requests for Confidential Financial Information;
- Unauthorized access to hard copy files or reports;

- Unauthorized transfer or release of Confidential Financial Information by third parties contracted by the University;
- Unauthorized disposal of Confidential Financial Information; and
- Unsecured disposal of Confidential Financial Information.

CUNY also recognizes that the foregoing may not be a complete list of risks associated with the protection of Confidential Financial Information. Since technology growth is not static, new risks are created regularly. Accordingly, the University will actively participate in and monitor advisory groups such as the *New York State Office of Cyber Security & Critical Infrastructure Coordination*, the *Educause Security Institute*, the *Internet2 Security Working Group,* the *U.S. Department of Homeland Security*, the *Carnegie Mellon Group,* and the *SANS Institute* to identify new risks. CUNY's Information Technology Security Committee (a sub-committee of the CUNY Information Technology Steering Committee) will actively seek to identify and address all potential technology security risks associated with Confidential Financial Information.

In addition, the University Office of Internal Audit and Management Services will incorporate continuous monitoring and identification of security risks and controls into its Annual Risk Assessment/Internal Control Review process.

III. Design and Implementation of a Safeguarding Program

CUNY's Information Security Program has four components: a) Employee Training and Management; b) Information System Security; c) Safeguarding Paper and Special Media Records; and d) Disposal of Records.

a. Employee Training and Management

Initially, all CUNY employees in departments that collect, access, retain, transmit or dispose of Confidential Financial Information (e.g., all employees involved in Perkins Student Loan processes) will receive a copy of this Information Security Program. Each director of a department covered by this Information Security Program is responsible for ensuring that all employees under his or her direction receive this document and for clarifying how the Information Security Program is applicable to the employees in his or her department. The Program Coordinators should ensure that each department director is aware of this responsibility. On an ongoing basis, each department director should ensure that all new employees in his or her department, whether new hires or transfers, receive a copy of this Information Security Program as part of the orientation to the department. The University Program Coordinator will arrange for training of the various groups impacted by the GLB Safeguards Rule throughout the University, as needed, on an ongoing basis.

b. Information System Security

Access to Confidential Financial Information through University and College networks and stand-alone systems should be limited to those employees who have a business reason to have such information. Each employee with access to Confidential Financial Information should be assigned a user name and password. Only employees with the need to have access to such

information should be provided passwords. All databases and imaged documents containing Confidential Financial Information should be password-protected.

CUNY will take reasonable and appropriate steps consistent with current technological developments to ensure that all Confidential Financial Information is secure and to safeguard the integrity of records in storage and transmission. These steps include maintaining CUNY's operating systems and applications and providing appropriate patches and updates in a timely manner. The University's Office of Computer and Information Services is evaluating the feasibility of implementing an intrusion detection system to detect and stop most external threats and is also developing a protocol to react to intrusions into the University and College networks.

To the extent reasonably available, CUNY should use encryption technology for both storage and transmission of all Confidential Financial Information. All Confidential Financial Information should be maintained on servers behind a University firewall. University and College Information Technology Departments should keep all firewall software and hardware current.

The CUNY Information Technology Security Committee will review and modify current policies and develop new policies to provide appropriate security to University and College information systems.

c. Safeguarding Paper and Special Media Records

Access to Confidential Financial Information should be restricted to CUNY employees with a legitimate business purpose and on a need-to-know basis. Whether this information is stored in hard copy form or in special media records, such as microfiche and microfilm, employees should exercise reasonable care for its safekeeping. (For example, records common to the Perkins Student Loan processes include documents collected during the verification process, entrance and exit interview documents, promissory notes, and hard copy reports. Proper treatment of these records should follow established standards, procedures and techniques governing good record-keeping practices. The records should be kept in lockable file cabinets, and promissory notes must be secured in a locked fireproof container in accordance with federal regulations.) All records containing Confidential Financial Information should be handled only by authorized personnel and kept in areas with restricted access. Such records should not be left open on desks if unattended for extended periods of time. Supervisory staff should periodically test and monitor the effectiveness of these safeguards to ensure that they are working as intended.

d. Disposal of Records

Stored records should be maintained until they become inactive or are no longer required under applicable rules and regulations. When no longer active or required, records should be destroyed or retired in accordance with CUNY's published schedules governing the disposition of such records. Paper and microfilm, microfiche and other special media records that are no longer required to be kept by the University should be shredded at the time of disposal. Electronic documents should be deleted and magnetic media should be erased.

The designated Records Retention Officer at the University and at each College is responsible for administering a records management program and should be consulted with any questions about the disposition status of records.

IV. Oversight of Service Providers and Contracts

The GLB Safeguards Rule requires that the University take reasonable steps to select and retain service providers who will maintain safeguards to protect Confidential Financial Information. Contracts entered into on or before June 24, 2002 should be modified to include an appropriate commitment to safeguarding Confidential Financial Information by May 24, 2004. Contracts entered into after June 24, 2002 should be modified to include an appropriate commitment to safeguarding Confidential Financial Information as of May 23, 2003. Each Program Coordinator should work with the College's Office of Legal Affairs and/or the University's Office of the General Counsel to put such agreements into place.

V. Review and Revision of CUNY Information Security Program

The GLB Safeguards Rule mandates that this Information Security Program be subject to periodic review and adjustment. As information security technology evolves, the Information Security Officer at the University and at each College should constantly monitor the technology in place and make adjustments as necessary to preserve the infrastructure of CUNY's information systems.

Each Program Coordinator should annually reassess the areas other than information security technology covered by this Information Security Program in conjunction with the University Office of Internal Audit and Management Services. This assessment will be accomplished primarily through the Annual Risk Assessment/Internal Control Review process, which is intended to provide department directors with a mechanism to evaluate and assess their respective operations and control procedures.

Under this annual process, department directors at each College reassess their own operations and submit an Annual Risk Assessment/Internal Control Review report indicating any changes or modifications to the existing systems of internal control made during the year, the status of any planned improvements, the types of control testing, and, if applicable, any corrective changes taken. Under this process, the department directors also identify the type of training and the training provider for all formal training programs attended by members of their departments during the year as well as any topic or skill areas where additional training is needed. This annual assessment and review process should be used as the mechanism to re-evaluate existing information security safeguards and identify new processes that deal with information covered by the GLB Safeguards Rule.

Related Links

http://www.ftc.gov/os/2002/05/67fr36585.pdf - GLB Safeguards Rule (16 CFR Part 314)

http://portal.cuny.edu/cms/id/cuny/documents/informationpage/000814.htm - University Internal Control Program

http://portal.cuny.edu/cms/id/cuny/documents/level_3_page/001171.htm - University Computer Usage Policy

http://portal.cuny.edu - Security/Privacy Policy