Gramm-Leach Bliley Act (GLBA)
Financial Information Security Program Policy

Contents

PURPOSE/POLICY:

The Federal Trade Commission's Safeguards Rule, which implements the security provisions of the Gramm-Leach-Bliley Act (GLBA)/Program, went into effect on May 23, 2003. The Safeguards Rule requires financial institutions, which includes colleges and universities that are significantly engaged in providing Financial Services, to protect the security, confidentiality, and integrity of customer financial records, including non-public personally identifiable financial information. To ensure this protection, the GLBA Safeguards Rule mandates that all covered financial institutions establish appropriate administrative, technical and physical safeguards (Reference 16 CFR § 314.1(a)).

Therefore, any CUNY College, office or department that collects, stores or processes Covered Data must implement data protection standards in order to ensure compliance. This is in addition to any other University policies and procedures that may be required pursuant to federal and state laws and regulations, including the Family Educational Rights and Privacy Act (FERPA).

SCOPE:

This Policy applies to all CUNY 'colleges' as defined below. It may also apply to the University's Related Entities under certain circumstances which are defined in this Policy.

REASON FOR POLICY:

To ensure that individuals and departments that access or utilize Covered Data understand their responsibility with respect to GLBA compliance.

WHO SHOULD READ THE POLICY:

- Any individual or department that has access to Covered Data including but not limited to the following (GLBA Relevant Departments):
    - Enrollment Management (Recruiting, Admissions, Applications Processing, Registrar, Financial Aid)
    - Finance, Business Office, Bursar (and alternative collection points), Accounting, Accounts Payable, Vendor Management, Customer Management, Grants Management
    - Human Resources
    - Institutional Advancement
    - Adult and Continuing Education and Similar Programs and Offices
    - Student Affairs
    - Academic Affairs
    - Performing Arts Centers
    - Information Technology

OBJECTIVE OF THE PROGRAM:

- Protect the security and confidentiality of Covered Data;
- Protect against anticipated threats or hazards to the security or integrity of Covered Data; and
- Protect against unauthorized access to or use of Covered Data that could result in substantial harm or inconvenience to any Customer.

DEFINITIONS:

"College" means a constituent unit of the University, including without limitation senior and community colleges, graduate and professional schools, Macaulay Honors College and the Central Office, as well as fund groups and organizations that are not legally separate from the University (e.g., the Queens College Athletic and Recreational Fund and the college associations of Hunter College, the School of Professional Studies and the Graduate School of Public Health and Health Policy).

"Covered Data" means (i) non-public personal financial information about a Customer and (ii) any list, description, or other grouping of Customers (and publicly available information pertaining to them) that is derived using any non-public personal financial information. Examples of Covered Data include bank and credit card account numbers, income and credit histories, tax returns and social security numbers and lists of public information such as names, addresses and telephone numbers derived in whole or in part from personally identifiable financial information (e.g., names of students with outstanding loans). Covered Data is subject to the protections of GLBA, even if the Customer ultimately is not awarded any financial aid or provided with a credit extension.

Covered Data includes such information in any form, including paper and electronic records.

"CUNY" and **"University"** mean The City University of New York.

"Customer" means any individual (student, parent, faculty, staff, or other third party with whom the University interacts) who receives a Financial Service from the University for personal, family or household reasons that results in a continuing relationship with the University.

"Financial Service" includes offering or servicing student and employee loans, receiving income tax information from a student or a student's parent when offering a financial aid package, engaging in debt collection activities, and leasing real or personal property to individuals for their benefit.

"Related Entities" means the following types of entities and their subsidiaries, if legally separate from the University and unless otherwise indicated: auxiliary enterprise corporations, college associations, student services corporations, childcare centers, performing arts centers, and art galleries.

"Service Provider" means any person or entity that receives, maintains, processes, or otherwise is permitted access to Covered Data information through its direct provision of services to the University.

GLBA REQUIREMENTS:

The GLBA mandates that the University (i) designate an employee(s) to coordinate the Program, (ii) identify internal and external risks to the security and confidentiality of Covered Data and evaluate current safeguards, (iii) design and implement safeguards to control the identified risks and regularly test and monitor the effectiveness of these safeguards, (iv) oversee Service Providers and contracts, and (v) evaluate the information security program.

I. Designation of GLBA Program Coordinators:

The University Central Office shall designate an appropriate individual(s) to serve as the 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 GLBA Safeguards Rule and disseminating relevant information and updates.

In addition, the President of each College shall designate a College Program Coordinator for their campus.

II. Identification of Risks and Risk Assessment:

CUNY recognizes that there are both internal and external risks associated with the protection of Covered Data. These risks include, but are not limited to:

- Unauthorized access to Covered Data;
- Compromised system security as a result of system access by an unauthorized person;
- Interception of Covered Data during transmission;
- Loss of data integrity;
- Physical loss of Covered Data in a disaster;
- Errors introduced into the system;
- Corruption of data or systems;
- Unauthorized requests for Covered Data;
- Unauthorized access to hard copy files or reports containing Covered Data;
- Unauthorized transfer or release of Covered Data by third parties contracted by the University;
- Unauthorized disposal of Covered Data; and
- Unsecured disposal of Covered Data.

CUNY also recognizes that the aforementioned may not be a complete list of risks associated with the protection of Covered Data. Since technology changes over time, the possibility of new risks may arise. CUNY's data owners and custodians will actively seek to identify and address all potential technology security risks associated with Covered Data.

In addition, the University Office of Internal Audit shall 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:

a. Employee Training and Management

All CUNY employees in departments that collect, access, retain, transmit or dispose of Covered Data (GLBA Relevant Departments) will receive a copy of this Information Security Program. Each department director covered by this Information Security Program is responsible for ensuring that

all employees under their direction receive this document and for clarifying how the Information Security Program is applicable to the employees in their department. The College Program Coordinators shall ensure that each department director is aware of this responsibility. On an ongoing basis, each department director shall ensure that all new employees in their 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 and the College Program Coordinator will arrange for training of the various groups impacted by the GLBA Safeguards Rule throughout the University, as needed, on an ongoing basis.

b. Information System Security

Access to Covered Data through University and College networks and stand-alone systems shall be limited to those employees who have a business reason to have such information per IT Security Procedure requirements. Only employees with the need to have access to certain Covered Data shall be granted access to that data or be authorized to collect such data from Customers. All databases and imaged documents containing Covered Data must be appropriately protected, including use of password or other authentication, encryption and other access restrictions as appropriate.

While the University utilizes industry-standard protocols and cybersecurity technologies, including firewalls, intrusion prevention, encryption, anti-malware, email security and restricted physical access to its data centers to protect its digital assets, everyone's participation is required, in consultation with CUNY and College information technology departments, to ensure that reasonable and appropriate steps are taken to protect Covered Data and to safeguard the integrity of records in storage and transmission. These steps include maintaining operating systems and applications, applying security-related updates in a timely manner after appropriate testing and reviewing overall protections on an ongoing basis.

All Covered Data shall be handled with care and scrutiny and shall be protected and controlled, including but not limited to storage on University servers behind firewalls where applicable. If cloud storage and applications are to be used, then compliance with the 'Acceptable Use of University Data in the Cloud' policy is required. All University information security software and hardware protections shall be maintained with vendor support at current or higher levels. Sensitive data discovery and data loss prevention tools shall be utilized in areas of high risk to ensure that Covered Data is identified and protected as required.

At all times, Covered Data shall be maintained in a manner consistent with University policies and procedures, as detailed in CUNY IT Security Procedures at security.cuny.edu, including the General Procedures, Data Classification Standard and Acceptable Use of University Data in the Cloud. Encryption technology should be used for both storage and transmission of all Covered Data where possible. Encryption of Covered Data on mobile devices is required per IT Security Procedures.

Policies shall be periodically reviewed and modified, and new policies developed as needed, to define required security for University and College information systems.

c. Safeguarding Paper and Electronic Records

Access to Covered Data shall be limited to those employees who have a business reason to have such information per IT Security Procedure requirements. Whether this information is stored in hard copy form or electronically, employees must exercise appropriate care for its safekeeping by following these guidelines:

1. Safeguarding Paper Information

- ✓ Secure Covered Data by locking file cabinets and offices when not in use.
- ✓ Do not leave Covered Data unattended and unsecured.
- ✓ Access to Covered Data shall only be granted to those who need such access.
- ✓ Comply with other applicable University policies and procedures including, but not limited to, CUNY's Records Retention Schedule.

2. Safeguarding Electronic Information

- ✓ Password-protect computers and systems with access to Covered Data, and log off of computers and systems when access to Covered Data is no longer needed. Shut down and turn off computers at the end of each day where possible (when working remotely, this may not be possible).
- ✓ Do not leave Covered Data unattended and unsecured.
- ✓ Access to computers and systems shall only be granted to those who need such access.
- ✓ Encrypt Covered Data when transmitting or storing it electronically.
- ✓ Monitor systems for actual or attempted attacks, intrusions, or other systems failures.
- ✓ Comply with other applicable University policies and procedures including, but not limited to:
  - o CUNY's Information Security Policies & Procedures
  - o CUNY's Records Retention Schedule

d. Disposal of Records Containing Covered Data

Stored records containing Covered Data shall be maintained only until they become inactive or are no longer required under applicable rules and regulations. When no longer active or required, records shall be destroyed or retired in accordance with CUNY's Records Retention Schedule governing the disposition of such records. Paper records that are no longer required to be kept by the University shall be shredded at the time of disposal. Electronic documents shall be deleted and magnetic media shall 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 GLBA Safeguards Rule requires that the University take reasonable steps to select and retain Service Providers who will maintain safeguards to protect Covered Data. Appropriate steps shall be taken to ensure that all relevant contracts include a privacy clause, and that all existing contracts are in compliance with GLBA.

V. Program Review and Revision:

This program/policy is subject to review and revision to ensure compliance with current and future laws and regulations. With the exception of modifications, supplements or updates necessitated by changes in law, regulations or administrative requirements, or to ensure consistency with other

University policies, any proposed amendments to this Policy must be approved by the CUNY Board of Trustees. The CUNY Office of Budget and Finance will be responsible for the periodic review of this Policy, as well as ensuring that all appropriate parties are informed of them.

APPLICATION TO RELATED ENTITIES:

Any Related Entity that provides a Financial Service or assists the University or a College with the administration of a Financial Service shall comply with this policy as follows:

- Related Entities that maintain or distribute Covered Data relating to a Financial Service on or through a University server or other technology under University control, or which assist the University or a College with the administration of a Financial Service shall be deemed to be part of their supported College, solely for purposes of compliance with this policy.

- Related Entities that are subject to GLBA but maintain and/or distribute Covered Data relating to a Financial Service independent of any University-controlled technology and do not assist the University or a College with the administration of a Financial Service, shall adopt their own policy(ies) consistent with the requirements of GLBA and this policy, including without limitation regarding information system security, the training of employees, and safeguarding of information.

RELATED LINKS & RESOURCES:

Federal Trade Commission - Financial Institution and Customer Information: Complying with the Safeguards Rule - https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-informationcomplying

EDUCAUSE - https://er.educause.edu/articles/2018/10/the-glba-safeguards-rule-at-15

Office of Internal Audit
https://www.cuny.edu/about/administration/offices/office-of-risk-audit-and-compliance/oiams/

CUNY Information Security Policy
https://www2.cuny.edu/about/administration/offices/cis/information-security/security-policiesprocedures/

CUNY Record Retention Policy - https://policy.cuny.edu/schedule/

CUNY Breach Reporting Procedure - https://www2.cuny.edu/wp-content/uploads/sites/4/page-assets/about/administration/offices/cis/information-security/security-policiesprocedures/BreachReportingProcedureV07182006.pdf