RUTGERS
THE STATE UNIVERSITY
OF NEW JERSEY

RUTGERS POLICY

Section: 50.3.11

Section Title: Legal Matters

Policy Name: Gramm-Leach-Bliley Act (GLBA) Information Security Policy

Formerly Book: N/A

Approval Authority: Senior Vice President for Administration

Responsible Executive: Vice President for Information Technology and Chief Information Officer

Responsible Office: Office of Information Technology (OIT)

Originally Issued: August 19, 2008

Revisions: 10/10/2013 (Updated title)

Errors or changes? Contact: oitpolicy@rutgers.edu

1. **Policy Statement**
   It is the position of the university to provide safeguards to protect information and data in accordance with the Financial Services Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (GLBA). Therefore, any department that stores or processes customer financial information ("covered data") must implement data protection standards in order to ensure compliance.

2. **Reason for Policy**
   To ensure that individuals or departments that access or utilize covered data understand their responsibility with respect to complying with the GLBA.

   To identify the corresponding Rutgers standards that are to be implemented by owners and/or custodians of GLBA data.

3. **Who Should Read This Policy**
   University administrators including, but not limited to:
   - Chancellors and vice presidents
   - Deans, directors, chairs, and department heads
   - Administrators/managers

   All members of the Rutgers University community

4. **Related Documents**

GLBA Section 501 16 CRF Part 314
(May 23 Federal Register, p. 346484)
http://www.ftc.gov/os/2002/05/67fr36585.pdf

New Jersey Identity Theft Prevention Act, NJSA 56:8-161 through 56:8-166,
http://www.njleg.state.nj.us/2004/Bills/PL05/226_.HTM

50.3.9, Identity Theft Compliance Policy

Family Educational Rights and Privacy Act (FERPA),
http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

GLBA Control Standards
http://rusecure.rutgers.edu/policies-and-standards/glba-security-standards/

5. **Contacts**

Information Protection and Security, OIT
848-445-8011
rusecure@rutgers.edu

6. **The Policy**

50.3.11 GRAMM-LEACH-BLILEY ACT (GLBA) INFORMATION SECURITY POLICY

I. GLBA Requirements

Any person or department using or processing covered data shall ensure protection against anticipated threats or hazards to the security or integrity of covered data by implementing the GLBA control standards. Further, business units are responsible for ensuring that the following activities and processes are implemented:

A. Conduct an annual risk assessment of likely security and privacy risks.

B. Institute a training program for all employees who have access to covered data and information.

C. Oversee service providers and contracts to ensure the protection of covered data.

D. Evaluate and adjust their information security processes in light of testing and monitoring activities.

II. Definitions

"Covered data" means all information required to be protected under the Gramm-Leach-Bliley Act. "Covered data" also refers to financial information that the university, as a matter of policy, has included within the scope of the GLBA Information Security Program. Covered data includes information obtained from a student in the course of offering a financial product or service, or such information provided to the university from another institution. "Offering a financial product or service" includes offering student loans, receiving income tax information from current or prospective students and their parents as a part of a financial aid application, offering credit or interest bearing loans, and other miscellaneous financial services.

Examples of student financial information relating to such products or services are bank and credit card account numbers, income and credit histories, and social security numbers. "Covered

data" consists of both paper and electronic records that are handled by the university or its affiliates.

III. Roles and Responsibilities

The major responsibilities each party has in conjunction with the GLBA policy are as follows:

A. **GLBA Program Coordinator.** The Senior Vice President for Administration will designate a GLBA Program Coordinator to facilitate the GLBA compliance activities of the business units processing covered data. The coordinator, in conjunction with the Responsible Executive and the Responsible Office for this policy, will assist business units in meeting their obligations and responsibilities associated with protecting covered data, and corresponding policies and processes. Based upon the feedback collected from the business units, the coordinator will report on an annual basis the status of compliance, and communicate these findings to those with authority over the data.

The GLBA Program Coordinator will collect the status from all units and provide annual reports to the Executive Vice President for Academic Affairs, the Senior Vice President for Administration, and the Chancellors in Newark and Camden.

B. **University Administrators.** The university administrators responsible for managing employees with access to "covered data" are responsible for ensuring protection of covered data through the application of the GLBA control standards and required processes outlined in this document.

The university administrators will designate a responsible point of contact to work with the GLBA Program 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 their Information Security Program for covered data accessible in that unit to the GLBA Program Coordinator at least annually and more frequently where appropriate.

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

D. **Compliance with this Policy.** Departmental compliance with this policy is subject to review by the Office of the Vice President and General Counsel and the Internal Audit Department.

IV. Protection Standards

The GLBA Control Standards have been developed in order to provide direction on the appropriate logical, administrative, and physical security controls to apply to GLBA Data. Therefore, GLBA university data will be protected by implementing the GLBA Control Standards (see “Related Documents” above).