Skip to content. | Skip to navigation

- Site Map
- Accessibility
- Contact

Search Site

Advanced Search…

RUSecure

Sections

- Home
- RU Security News
- Students and Home Users
- Department IT Security
- Services
- NPPI
- Policies and Standards

Personal tools

- Log in

You are here: Home → Department IT Security → Technical Staff → Compliance → Gramm-Leach-Bliley Act (GLBA) → RU Compliance Policy In Support of GLBA

Document Actions

- 🖨

RU Compliance Policy In Support of GLBA

last modified 2007-07-27 11:28

Rutgers University GLBA Policy

Rutgers University Information Security Program

I. Purpose

In order to continue to protect private information and data, and to comply with new federal laws, the University has adopted this Information Security Program for certain highly critical and private financial and related information. This security program applies to customer financial information ("covered data") the University receives in the course of business as required by these new federal laws, as well as other confidential financial information the University has voluntarily chosen as a matter of policy to include within its scope. This document describes many of the activities the University currently undertakes, and will undertake, to maintain covered data according to legal and University requirements. This Information Security Program document is designed to provide an outline of the safeguards that apply to this information. The practices set forth in this document will be carried out by and impact diverse areas of the University.

II. Definitions

"Covered data" means all information required to

be protected under the Gramm-Leach-Bliley Act (GLBA). "Covered data" also refers to financial information that the University, as a matter of policy, has included within the scope of this 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 a current or prospective student's parents as a part of a financial aid application, offering credit or interest bearing loans, and other miscellaneous financial services as defined in 12 CFR § 225.28. 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.

"Service Providers" refers to all third parties who, in the ordinary course of University business, are provided access to covered data. Service providers may include businesses retained to transport and dispose of covered data, collection agencies, and systems support providers, for example.

III. Security Program Components

The GLBA requires the University to develop, implement and maintain a comprehensive information security program containing the administrative, technical and physical safeguards that are appropriate based upon the University'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, and (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.

IV. Security Program Coordinator

The Security Program Coordinator ("Coordinator) will be responsible for coordinating the implementation of this Information Security Program. The Coordinator is presently the OIT-ESS Director for Information Protection and Security. The Director, OIT-ESS-IPS will work closely with the Financial Aid offices on all campuses, The Controller's office, the Office of Compliance and Student Policy Concerns, the Office of University Counsel, Internal Audit, University Athletic Office, OIT-ESS-Administrative Computing Services, and other offices and units to implement this program. The Coordinator will consult with responsible offices to identify units and areas of the University 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 University with access to covered data. The Coordinator will ensure that departments self-report their compliance with risk assessments and system standards and monitoring, as set forth in sections V and VI. Also, the Coordinator will periodically conduct vulnerability assessments of units to ensure compliance. The Coordinator may require units with substantial access to covered data to

further develop and implement comprehensive security plans specific to those units and to provide copies of the plan documents. The Coordinator may designate, as appropriate, responsible parties in each area or unit to carry out activities necessary to implement this Information Security Program.

The Coordinator will work with responsible parties to ensure that the departmental training and education plans are developed and delivered for all employees with access to covered data. The Coordinator will, in consultation with other University 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 prepare an annual report on the status of the Information Security Program and provide that to the University's Cabinet. The Coordinator may prepare more frequent reports as necessary or as requested. These reports may include copies of any unit-specific security plans, current risk assessments for each unit with access to covered data, statements on the controls in place to mitigate those risks and the effectiveness of those controls, summaries of monitoring activities, actions taken or to be taken to correct any security concerns identified through monitoring, and such other information as required to provide assurance that this Information Security Program is implemented and maintained.

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 containing the elements set forth above in Section III at all times and make the plan available to the

University community.

V. 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 otherwise compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. Risk assessments will include consideration of risks in each area that has access to covered information. Risk assessments will include, but not be limited to, consideration of employee training and management; information systems, including network and software design, as well as information processing, storage, transmission and disposal; and systems for detecting, preventing, and responding to attacks, intrusions, or other system failures.

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. The Coordinator will ensure that risk assessments are conducted at least annually, and more frequently where required. The Coordinator may identify a responsible party from the Rutgers University Computing Services to conduct the system-wide risk assessment. The Coordinator may identify a responsible party in each unit with access to covered data to conduct the risk assessment considering the factors set forth above, or employ other reasonable means to identify risks to the security, confidentiality and integrity of covered data in each area of the University with covered data.

The Coordinator will provide copies of complete and current risk assessments for system-wide and

unit-specific risks at least annually with the Coordinator's report to the University Cabinet. Any risk assessments completed by the Coordinator and the Office of Information Technology are incorporated to and made part of this document.

VI. 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 in Section V. The Coordinator will work with departments to 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 University has adopted comprehensive policies, standards and guidelines setting forth the procedures and recommendations for preserving the security of private information, including covered data. These are set forth in Section X.

The Coordinator will, working with other responsible offices and units, help to identify categories of employees or others who have access to covered data. The responsibility for employee training will reside with the departments. Each department will be responsible for developing training materials and identifying a core set of trainers within each department. Such training will include education on relevant polices and procedures and other safeguards in place or developed to protect covered data. Training and education may also include

Contact information

rusecure@rutgers.edu
(732) 445-8011
abuse@rutgers.edu

RU Secure Home

- ❍ Gramm-Leach-Bliley Act (GLBA)
- ❍ RU Compliance Policy In Support of GLBA
- ❍ GLBA Security Program-Annual Report
- ❍ GLBA Security Program-Planning
- ❍ GLBA Security Program-Training
- ❍ GLBA Security Program-Prevention
- ❍ GLBA Security Program-Detection
- ❍ GLBA Security Program-Reaction/Recovery

GLBA Security Program-Reporting

○

GLBA Annual Report (Expanded)

newsletters, promotions or other programs to increase awareness of the importance preserving the confidentiality and security of confidential data. Department heads will report annual training status to the program Coordinator.

Other safeguards will also be used, as appropriate, including job-specific training on maintaining security and confidentiality, requiring user-specific passwords and required periodic changes to those passwords, limiting access to covered data to those with a business need for access to information, requiring signed certification of responsibilities prior to authorizing access to systems with covered data, requiring signed releases for disclosure of covered data, establishing methods for prompt reporting of loss or theft of covered data or media upon which covered data may be stored, and other measures that provide reasonable safeguards based upon the risks identified.

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.

Safeguards for information processing, storage, transmission, retrieval and disposal may include: requiring electronic covered data be entered into a secure, password-protected system; using secure connections to transmit data outside the University; using secure servers; ensuring

covered data is not stored on transportable media (floppy drives, zip drives, etc); permanently erasing covered data from computers, diskettes, magnetic tapes, hard drives, or other electronic media before re-selling, transferring, recycling, or disposing of them; storing physical records in a secure area and limiting access to that area; providing safeguards to protect covered data and systems from physical hazards such as fire or water damage; disposing of outdated records under a document disposal policy; shredding confidential paper records before disposal; maintaining an inventory of servers or computers with covered data; and other reasonable measures to secure covered data during its life cycle in the University's possession or control.

C. Managing System Failures

The University will maintain effective systems to prevent, detect, and respond to attacks, intrusions and other system failures. Such systems may include maintaining and implementing current anti-virus software; checking with software vendors and others to regularly obtain and install patches to correct software vulnerabilities; maintaining appropriate filtering or firewall technologies; alerting those with access to covered data of threats to security; imaging documents and shredding paper copies; backing up data regularly and storing back up information off site, as well as other reasonable measures to protect the integrity and safety of information systems.

Departments discovering a compromise of covered data are required to report this information to abuse@rutgers.edu with as much information as possible.

D. Monitoring and Testing

Monitoring systems will be implemented to regularly test and monitor the effectiveness of information security safeguards. Monitoring will be conducted to reasonably ensure that safeguards are being followed, and to swiftly detect and correct breakdowns in security. The level of monitoring will be appropriate based upon the potential impact and probability of the risks identified, as well as the sensitivity of the information provided. Monitoring may include sampling, system checks, reports of access to systems, reviews of logs, audits, and any other reasonable measures adequate to verify that Information Security Program's controls, systems and procedures are working.

E. Reporting

The Coordinator will provide a report on the status of the information safeguards and monitoring implemented for covered data as described in Section IV.

VII. Service Providers

In the course of business, the University may from time to time appropriately share covered data with third parties. Such activities may include collection activities, transmission of documents, 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 the Office of General Counsel, the University Procurement office and other offices as appropriate, to make certain that service provider contracts contain appropriate terms to protect the security of covered data.

VIII. 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 in Section VI, as well as any material changes to operations or business arrangements, and any other circumstances which may reasonably have an impact on the Information Security Program.

The Coordinator and the University's Vice-President for Information Technology will review this Information Security Program document at least annually.

IX. Roles and Responsibilities

Provosts' Offices, Deans, Director, Department Heads and other Managers. The Provost, dean, department head, director or other manager responsible for managing employees with access to "covered data" will designate a responsible point of 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 at least annually, and more frequently where appropriate.

The Provost, dean, department head, director or other manager will designate individuals who

have the responsibility and authority for information technology resources; establish and disseminate enforceable rules regarding access to and acceptable use of information technology resources; establish reasonable security policies and measures to protect data and systems; monitor and manage system resource usage; investigate problems and alleged violations of University information technology policies; and refer violations to appropriate University offices such as the Office of the General Counsel, Deans, Department heads, and the University Police Department where criminal activity is suspected for resolution or disciplinary action.

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.

Security Program Coordinator. The Security Program Coordinator is responsible for coordinating the implementation of the provisions of this Information Security Plan.

University Counsel and the Internal Audit Department. Departmental compliance with this policy is subject to review by University Counsel and the Internal Audit Department.

X. Policies, Standards and Guidelines

The University has adopted comprehensive policies, standards, and guidelines relating to information security. http://oit.rutgers.edu/policies.html They are incorporated by reference into this Information Security Plan, and include:

Policies

Acceptable Use of Information Technology Resources

Security Requirements

Privacy

Data Access Policy

Network-Related Policies

NetID/Email Address Policy

Standards for management of computer systems

Wireless LAN policy

Standards for University Operations Handbook

Other Policies

Public Access to University Information http://records.rutgers.edu/

[Powered by Plone CMS, the Open Source Content Management System](#)

This site conforms to the following standards:

- [Section 508](#)
- [WCAG](#)
- [Valid XHTML](#)
- [Valid CSS](#)
- [Usable in any browser](#)