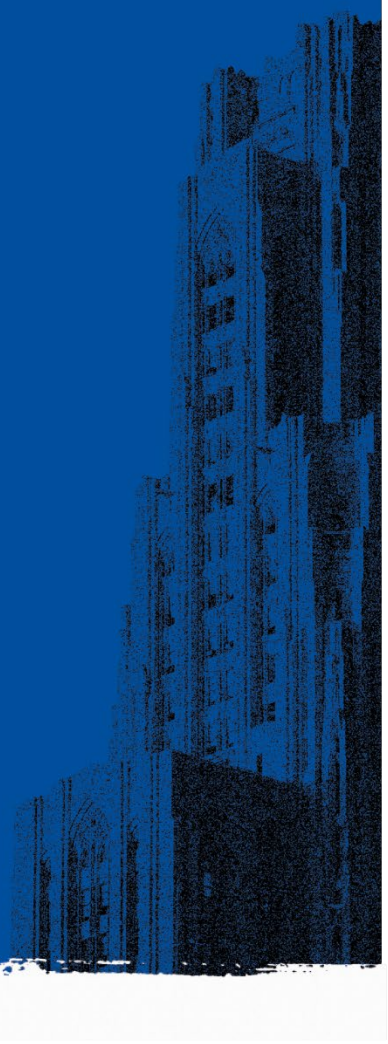
University of Pittsburgh

GLBA Information Security Program



University of Pittsburgh

Office of Compliance, Investigations & Ethics
https://compliance.pitt.edu
(412) 383-4553

Pitt IT Security
https://www.technology.pitt.edu/security

GLBA INFORMATION SECURITY PROGRAM

Overview of Requirements

The Gramm-Leach-Bliley Act (GLBA) is administered by the Federal Trade Commission, who oversees regulation and enforcement of the Act. The goal of the Act is to ensure the security and confidentiality of customer information. The Act requires financial institutions to explain their information-sharing practices to customers and to safeguard sensitive data.

The Federal Trade Commission considers most institutions that participate in the Department of Education's student financial assistance program as "financial institutions" and accordingly, subject to the Act. The University must therefore comply with GLBA; specifically, by ensuring that all federal student aid applicant information is protected from access by or disclosure to unauthorized personnel.

Under Title IV of the Higher Education Act of 1965, the University is required to both assess and implement strong security policies and controls, as well as undertake ongoing monitoring and management for the systems, databases and processes that support the administration of Federal student financial aid. Such systems, databases, and processes include all systems that collect, process, and distribute information in support of applications for and receipt of Title IV student assistance.

The goal of this Program is to provide clear guidance and support for those individuals and departments responsible for:

- Ensuring the security and confidentiality of student information;
- Protecting against anticipated threats to the security and integrity of student information; and
- Protecting against unauthorized access to or use of such information that could result in harm or inconvenience to any student.

I. Designation of Responsibility

Coordination of Information Security Program. The University's Assistant Vice Chancellor for Compliance, Investigations & Ethics and the Chief Privacy Officer serves as the University's Privacy Officer and oversees the University's compliance with GLBA. The University's Privacy Officer works closely with Pitt IT Security to conduct and review annual assessments, discussed in greater detail below. The Office of Compliance, Investigations & Ethics also serves as a resource to the University community with respect to privacy of all its constituents and customers.

II. Identification of Responsible Departments

The University has identified Student Financial Services and the Office of Admissions and Financial Aid (OAFA) for all campuses as the units responsible for the administration of Title IV Federal student financial aid programs. A list of employees who have access to student financial aid data as a requirement of their position is maintained and regularly audited by Pitt IT.

III. Annual Assessments

On an annual basis, Pitt IT Security requires responsible departments to complete a Customer Information Security Plan (CISP). The Senior Security Analyst and CISP Program Coordinator for Pitt IT Security oversees the CISP program. CISPs are due by June of each year. The questions in the CISP are designed to capture data associated with information systems, network and software design, as well as information processing, storage, transmission, and disposal. Also included are additional questions that relate to how data is monitored, incident response plans and disaster recovery plans for each department. Pitt IT security regularly monitors the needs of the university and reworks the questions on the CISP as needed.

The University also conducts annual user audits of the PeopleSoft system, which houses student record information, including financial data, as well as a risk assessment of the vendor who hosts PeopleSoft.

IV. Safeguards

After reviewing the CISP responses from responsible departments and the annual audit results, the University's Privacy Officer, the Office of Compliance, Investigations & Ethics and Pitt IT Security work collaboratively to ensure that appropriate safeguards are in place.

Ongoing Security Support. Pitt IT Security monitors the University's network to identify potential security threats and quickly responds to security issues related to customer information. Specific to the PeopleSoft system, Pitt IT Security notes the following:

- User access to PeopleSoft and financial aid data requires business justification, review, and approval by a designated data steward
- User access to PeopleSoft and financial aid data is audited annually in coordination with data stewards
- The vendor hosting the PeopleSoft application and infrastructure on behalf of the University undergoes annual data security reviews by Pitt IT Security

Other relevant services provided by Pitt IT Security include:

- Controlling access to the University network and enterprise applications containing customer information with firewalls and access control lists.
- Installing centrally managed anti-virus software on endpoints to detect potentially malicious code rapidly.
- Aggregating security-related logs from endpoints, firewalls, anti-virus tools, and other network devices into Splunk for further threat detection and analysis.
- Performing vulnerability scanning on the University's internal data center that supports enterprise applications handling GLBA information.
- Immediately responding to all security incidents reported by any department, including those who possess GLBA covered data.
- Conducting security reviews of all third-party vendors that handle GLBA data.

V. Annual Training

Pitt IT security offers training on Security Awareness and GLBA content for all responsible departments. The designated security person for the CISP in each responsible department is required to complete security awareness training, and employees with access to financial aid data within PeopleSoft annually complete the training.

Pitt IT monitors training compliance through the KnowBe4 training platform.

VI. Cyber Incident and Security Event Planning

The University maintains and annually updates its Cyber Incident Response Plan (CIRP). The CIRP includes incidents that GLBA's Safeguard Rule describes as a "security event." A security event for GLBA purposes is an episode resulting in

unauthorized access to or misuse of information stored on the University's computing network or maintained in physical form.
University members who detect a security incident should contact Pitt IT Security using the 24/7 Pitt IT Help Desk. Pitt IT Security will assist with initiation of the CIRP. Departments responsible for the information security program are provided with the CIRP and agree to comply with its terms.

VII. Annual Reporting

The Office of Compliance, Investigations & Ethics and Pitt IT Security provide an annual written report to the Senior Vice Chancellor and Chief Legal Officer, the Senior Vice Chancellor and Chief Financial Officer, and the Vice Chancellor and Chief Information Officer. The annual report includes an overall assessment of the University's compliance with this Program and a summary of risk management, audit results, security events, and any recommendations for changes to the Program. Also on an annual basis, the Office of Compliance, Investigations & Ethics reports to the Risk and Compliance Committee of the University's Board of Trustees regarding the University's compliance with this program.