Pittsburg State University Policies and Procedures

GLBA Compliance Program

Security Program Coordinator: Amanda Williams, ITS Security Officer

GLBA Security Committee Members: Amanda Williams, ITS Security Officer
Rachel Cameron, Controller
Amberly Downs, Asst. Director of Cashiers & Student Accounts
Michael Woodrum, Asst. Dir. of Student Financial Assistance
Scott Donaldson, Director of Student Financial Assistance
Melinda Roelfs, Registrar
Lori Scott-Dreiling, Director of Human Resources
Vacant Position, Internal Auditor

Purpose:

This document outlines Pittsburg State University's (the University) program to protect customer information and data and to comply with Federal Laws that apply to student financial information. The goal of this document is to define the University's Gramm-Leach-Bliley (GLB Act) Student Financial Information Security Program, to provide an outline to assure ongoing compliance with federal regulations related to the Program, and to enhance the University's ability to respond to likely future privacy and security regulations. While not limited to the following, these offices are known to be affected: Student Financial Assistance, Controller's Office, Registrar's Office, Cashiers & Student Accounts, Human Resources and Information Technology Services.

Scope:

The GLB Act, effective May 23, 2003, along with agreements between Pittsburg State University (the University), the United States Department of Education (Federal Student Aid Program Participation

Agreement – PPA, and the Student Aid Internet Gateway Enrollment Agreement – SAIG), and the Family Educational Rights and Privacy Act (FERPA) addresses the safeguarding privacy, security, and confidentiality of customer information and data, which includes student financial aid records and information. Educational entities that engage in financial activities, such as processing student loans, are required to comply. The GLB Act and other pertinent legislation outlines standards of care for information security across all areas of data management practices both electronic and physical (employee, student, customer, alumni, donor, etc.). Therefore, the University must safeguard all personally identifiable financial records and information regardless of where it resides and covers employees and all other individuals or entities using these records and information for any reason.

Categories of Information under the Program:

Information covered under the program is defined by three categories:

- Personal Identifiable Information (PII)– Also known as protected data, PII includes first and last name, social security number, date of birth, home address, home telephone number, academic performance record, physical description, medical history, disciplinary history, gender, and ethnicity.
- Financial Information – Information that the University has obtained from faculty, staff, students, alumni, auxiliary agencies and patrons in the process of offering financial aid or conducting a program. Examples include bank and credit card account numbers, and income and credit histories.
- Student Financial Information – Information that the University has obtained from a student in the process of offering a financial product or service, or such information provided to the University by another financial institution. Examples include student loans, income tax information received from a student's parent when offering a financial aid package, bank and credit card account numbers, and income and credit histories.

Departments and Documents Subject to Safeguard Guidelines:

Department Responsible	Protected Information
Student Financial Assistance Cashiers and Student Accounts Admission's Office Registrar's Office International Programs and Services Departmental Offices	• Student loans (university loans, bank loans, and federal loans) • Private Student loans • Personal Identifiable Information - SSN, Billing Information, Credit Card, Account Balance, Citizenship, Passport Information, Tax Return Information, Bank Account Information, Driver's License and Date of Birth • Disbursement of Financial Aid • Payment Plans • 1098-T
Human Resource Services (HRS)	• Personal Identifiable Information - SSN, Billing Information, Credit Card, Account Balance, Citizenship, Passport Information, Tax Return Information, Bank Account Information, Driver's License and Date of Birth • Payroll W2s • W-4 Payroll W2s
Business Office Purchasing Office	• Personal Identifiable Information - SSN, Billing Information, Credit Card, Account Balance, Passport Information, Tax Return Information, Bank Account Information, Driver's License and Date of Birth • G5 drawdown of federal funds • Employee Expense reimbursements • Reconciliations • Coordination of Audits • 1099 • W-9, W-8BEN

Policy:

This Program ensures that administrative, technical and physical safeguards are implemented by The University to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle covered data and information in compliance with the GLB Act. These safeguards are provided to:

- Ensure the security and confidentiality of covered data and information;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of covered data and information that could result in substantial harm or inconvenience to any customer.

The University shall appoint an Information Security Program Coordinator(s), conduct risk assessments of likely security and privacy risks, maintain a training program for all employees who have access to covered data and information, oversee service providers and contracts, and evaluate and adjust the Information Security Program as needed on an annual basis.

Procedure:

I. Employee Responsibilities and Access:

The following restrictions apply to all personally identifiable financial records and information maintained by the university and are meant to safeguard the security of these records and to maximize the integrity of the information. University employees are responsible for ensuring that, within their areas of responsibility, appropriate enforcement of the GLB Act program will be maintained.

- University employees are granted access to those data and information resources required to carry out the responsibilities of their position and may not access additional resources

without authorization (in other words, employees may not access customer information unless they have a need to know that information to perform their job duties).

- Access is determined based on the duties and responsibilities of each position and each employee is responsible for protecting their means of access from misuse. (for example, employees must not share their user name/password(s) with anyone else, or allow others to have access to their keys, etc.).
- Employees shall not knowingly alter, destroy, or misuse customer information.
- Employees must ensure that any release of customer information is conducted in an appropriate and secure manner (for example, employees should not release customer information without verifying the identity of the person(s) requesting the information, employees should use password protected file attachments and/or encrypted emails when transmitting confidential information, etc.).

II. Security Requirements:

Personally identifiable financial records and information, regardless of where it resides, must be maintained in a physically secure location with controlled access. Centralized and departmental computers and servers must have the appropriate level of physical and electronic security. The level of such security measures depends on the sensitivity of the data they process.

III. Risk Assessment:

This Committee will perform an annual risk assessment for the University. The risk assessment will include all GLB Act requirements. The Committee will work with all relevant areas of the University to identify potential and actual risks to the security and privacy of the systems that contain student financial information.

IV. Training Requirements

Each department subject to this program must complete the required GLB Act training. Department heads are responsible for ensuring that personnel are appropriately trained. Information security awareness training is also required for all staff working in GLB Act affected offices.

V. Service Provider Arrangements:

In the event the university contracts with a service provider to perform an activity in connection with any personally identifiable financial records and information, the University will take the following steps to ensure that the service provider performs its contracted activities in a secure manner:

- Require that service providers have reasonable policies and procedures in place to insure the security and confidentiality of customer records and information; and
- Require by contract, that all contracts with service providers contain language requiring the service providers to implement appropriate measures designed to ensure that customer information is kept confidential and that it is only used for the purposes set forth in the contract.

Definitions:

The following definitions apply to this program:

Customer: an individual who has obtained a financial product or service from the university to be used primarily for personal, family or household purposes and who has a continuing relationship with the university. Examples of activities which create customer relationships with the university could include obtaining a loan from the university or having a loan for which the university has servicing rights or responsibility.

Customer Information: non-public personal information about an individual who has obtained a financial product or service from the university for personal, family or household reasons, that results in a continuing relationship with the university. Examples would be any extension of credit by the university for household, personal or family purposes, such as an extension of credit for tuition, fees, housing, medical services, etc; the making and/or servicing of loans and/or financial aid. These situations are subject to the GLB Act, even if the individual ultimately is not awarded any financial aid or provided with a credit extension, in which case their non-public personal information would still be protected under the GLB Act.

Contact Information:

Persons who may have questions regarding the security of any of the categories of information that is handled or maintained by or on behalf of the University may contact:

Amanda Williams, ITS Security Officer
Pittsburg State University Information Technology Services
157K Kelce Center
Pittsburg, KS 66762
Email: akwilliams@pittstate.edu
Telephone: 620-235-4657

Rachel Cameron, Controller
Pittsburg State University Business Office
110 F Russ Hall
Pittsburg, KS 66762
Email: rcameron@pittstate.edu
Telephone: 620-235-4152

Scott Donaldson, Director of Student Financial Assistance
Pittsburg State University Student Financial Assistance
107 Horace Mann
Pittsburg, KS 66762
Email: scottdonaldson@pittstate.edu
Telephone: 620-235-4226

Michael Woodrum, Asst. Director of Student Financial Assistance
Pittsburg State University Student Financial Assistance

103 C Horace Mann
Pittsburg, KS 66762
Email: mwoodrum@pittstate.edu
Telephone: 620-235-4242

Amberly Downs, Asst. Director of Cashiers & Student Accounts
Pittsburg State University Cashiers & Student Accounts Office
112 C Horace Mann
Pittsburg, KS 66762
Email: adowns@pittstate.edu
Telephone: 620-235-4153

Melinda Roelfs, Registrar
Pittsburg State University Registrar's Office
103 D Russ Hall
Pittsburg, KS 66762
Email: mroelfs@pittstate.edu
Telephone: 620-235-4205

Lori Scott-Dreiling, Director of Human Resources
Pittsburg State University Human Resources Office
204 B Russ Hall
Pittsburg, KS 66762
Email: ldreiling@pittstate.edu
Telephone: 620-235-4118

Vacant Position, Director of Internal Audit
Pittsburg State University Internal Audit
219 B Russ Hall
Pittsburg, KS 66762
Email:
Telephone: 620-235-6167