Pacific University
Financial Information Security Program
Gramm-Leach-Bliley Act

Overview: This document summarizes Pacific University's comprehensive written financial information security program (the "Program") mandated by the Federal Trade Commission's Safeguarding Rule under the Gramm-Leach-Bliley Act (GLBA).

The Federal Trade Commission (FTC) requires that "financial institutions," which include most institutions for higher education establish policies and procedures for safeguarding customer financial information.[1] The GLBA also includes specific requirements regarding the privacy of customer financial information. The FTC has determined that education institutions that are in compliance with the Family Educational Rights and Privacy Act (FERPA) satisfy the privacy requirement of the GLBA. Educational institutions must, however, implement a safeguarding program. This procedure focuses on the FTC's safeguarding program requirement.

Designation of Representative(s): The Institution's Controller is designated as the Program Officer who is responsible for coordinating and overseeing the Program. The Program Officer may designate other representatives of the Institution to oversee and coordinate particular elements of the Program. Questions regarding implementation or interpretation of the Program should be directed to the Program Officer or his or her designee(s).

Program Objectives:

- Protect the security and confidentiality of customer records and information
- Identify and assess the risks to customer information in each relevant area and evaluate the effectiveness of the current safeguards for controlling these risks
- Select appropriate service providers and contract with them to implement safeguards
- Evaluate, test and monitor the Program and make changes as necessary

Risk Assessment:

The following is a list of potential threats to customer financial information that the Program is intended to mitigate.

1) Unauthorized access to data through software applications
2) Unauthorized use of another information system user's account and password
3) Unauthorized viewing of printed or computer displayed customer financial information
4) Improper storage of printed customer financial data information
5) Improper destruction of printed material that contains customer financial information

[1] Please note, the definition of a customer is anyone about whom the University collects, views, or keeps any type of financial information. Customers can be students, parents of students (or other relatives), employees, vendors, and/or members of the Board of Trustees.

Financial Information Security Program Components:

1. Access to the University's information system, Datatel, is limited to authorized personnel. Authorized personnel are assigned a username and two passwords to gain access to the information system. Approval for access to the various modules in the Datatel system is given by different managers. For example, access to the Financial Aid module requires the Financial Aid Director's approval and access to the Colleague Financial module requires authorization by the Controller. All managers/supervisors are required to review Datatel access of their staff members on an annual basis. Each manager who authorizes Datatel access to employees they do not directly supervise, must also annually review and approve continued access.

2. Passwords may not be shared.

3. Students requiring access to customer financial information are given their own account and password with appropriate privileges assigned.

4. Computer terminals used to display customer financial information are not to be left unattended with customer financial information displayed.

5. In unsecured areas, all users must log off their computer terminals when they are away from their work area.

6. Computer terminals are to be placed to prevent casual viewing by unauthorized personnel.

7. Entry access to the Business Office, Financial Aid Office, Registrar's Office, and other offices in Marsh Hall is limited to authorized personnel. Each University building has a designated person who approves key access for that particular building. Employees requesting a key must have a key request form signed by their supervisor and designated building person. Once approval is granted, keys can be picked up from the Facilities Office. The Facilities Office keeps a list on file of authorized key holders.

8. Printed copies of customer financial information are to be handled only by authorized personnel and kept in areas with restricted access.

9. Printed financial documentation and information of customers (including, but not limited to, credit card information, social security information, including social security numbers, bank information, loan information, salary and other personal financial information) must be kept secured at all times. This type of information cannot be left in full view of unauthorized individuals. Records with customer financial information are located in a number of areas, including, but not limited to, filing cabinets, folders, information from emails, information from phone calls whether verbal or written, binders, cash drawers, credit card machines, information in computer documents. Access to these areas is limited to authorized personnel.

10. Customer financial information, regardless of where the information is housed or how it is kept (in computer systems/programs, email, paper copies, etc.), is confidential and is not available to anyone except those who have a legitimate purpose for the information that is related to the University's mission. The following are examples of customer financial information that is confidential. This is not all inclusive:

    - Salary and benefit information for an employee
    - Wage information for students
    - Social Security Numbers (employees, students, vendors, etc.)
    - Credit Card Information
    - Loan Information
    - Bank Information
    - Dates of Birth
    - Home addresses and phone numbers

11. Printed customer financial information that is no longer needed must be placed in the Shred-it receptacle. In the Business Office, if the receptacle needs to be opened to retrieve discarded information, access can **ONLY** be approved by the Controller or Assistant Controller. Contents of the Shred-It receptacle can only be picked up by an authorized Shred-It representative. All other offices (Financial Aid, Registrar's Office and other offices) must have similar procedures regarding destruction of printed confidential customer financial information.

12. Offices must be kept locked when unattended or unsupervised.

13. Fraudulent attempts to obtain information will be reported to the appropriate office/individual.

Consequences: Disciplinary measures up to and including termination, may be imposed for breaches of the security components of this Program.

Employee Management and Training: The University will check references before hiring new employees. New employees gaining access to the University's information system will be asked to sign an agreement to keep student information confidential. In addition, each new employee working in an area where customer financial information is available, must sign a copy of this document indicating their agreement to keep financial information secured. Students working in these areas must be reminded of their obligation to keep information confidential, and must sign this statement.

Information Systems Management and Failures: The University Information Services Office (UIS) will provide effective security management to prevent, detect and respond to attacks of intrusion or other system failures. UIS provides the following security measures:

- Maintain up-to-date firewalls
- Provide appropriate anti-virus software that can be updated automatically
- Keep the information system updated with patches, new releases, etc., as appropriate

- Back-up customer information daily and keep weekly back-ups off site at a secured location and protected against destruction or damage
- Allow only approved users access
- Notify users about any security risks or breaches
- Use a password-protected system
- When transferring data from one computer to another, erase data from former computer
- Maintain an inventory of servers
- Maintain an inventory of user access

Monitoring and Testing: This Program must be reviewed periodically and adjusted when necessary. The most frequent of these reviews should occur within the UIS department, which will monitor software updates and new releases for security software and implement appropriate upgrades and new releases in a timely fashion. In addition, the University should hold meetings at least annually with appropriate employees to review the effectiveness of the Program and revise as necessary.

Please read and sign the following statement:

I have read Pacific University's Financial Information Security Program. I understand that I am required to keep all customer financial information private and not release information without customer approval. I will follow the Program's requirements and I understand that the University may take action against me, including termination of employment, if I breach this promise. If at anytime I have questions about the release of information or any aspect of this Program, I will contact my supervisor for assistance.

_____	_____	_____
Name	**Department**	**Date**