

# INFORMATION SECURITY PROGRAM

## Table of Contents

1. Overview
2. Scope of Covered Data
3. Related Policies
4. Security Program Components
5. Security Program Coordinator
6. Security Risk Assessment
7. Information Safeguards and Monitoring
  - a) Employee Management and Training
  - b) Physical Security
  - c) Computer System Security and Safeguard Failures
  - d) Monitoring and Testing
8. Service Providers
9. Continuing Evaluation and Adjustment

## 1. Overview

Effective May 23, 2003, the Federal Trade Commission (FTC), issued its final safeguards rules, as required by section 501(b) of the Gramm-Leach-Bliley Act (GLBA). The Federal Trade Commission (FTC) confirmed that higher education institutions are considered financial institutions under this federal law. The (FTC) promulgated the GLBA Safeguards Rule, 16 CFR Part 314, which requires higher education institutions to have an information security program containing reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of nonpublic personal customer information (covered data). These safeguards or elements are provided to:

- a) Ensure the security and confidentiality of covered records;
- b) Protect against any anticipated threats or hazards to the security of such records, and
- c) Protect against the unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to University customers.

## 2. Scope of Nonpublic Personal Customer Information

Or "covered data", means any personal identifiable financial or other personal information, not otherwise made publically available, that the University has obtained from a student, parent or customer in the process of offering a financial product or service. Covered data may also include personal information that the University obtained from an employee. Personal identifiable financial information includes names, date of birth, addresses, telephone numbers, bank and credit card account numbers, driver license, income and credit histories, social security numbers, and other financial tax information, both in paper and electronic form. Covered data also refers to checks that are handled in departments of the University in the course of business and other identifiable personal/private information such as medical records, educational records, and studies or surveys using personable identifiable data.

## 3. Related Policies, Procedures and Best Practices

The Information Security Program builds upon the WWU Code of Responsibility for Security and Confidentiality of Records and Files, Security and Data

Management WWU Best Practices and Policies, and Information Security Access Policy while incorporating other existing WWU policies, procedures and best practices that address various aspects of information privacy and security, including but not limited to:

- POL-U5300.01 Safeguarding Non-Public Financial Information, in compliance with the Family Educational Rights and Privacy Act (FERPA), and Gramm-Leach-Bliley Act (GLBA)
- POL-U5310.02 Defining Endowment Investment Objectives
- POL-U5351.01 Accepting and Maintaining Cash Receipting Locations
- POL-U5351.02 Training Cash Handlers
- POL-U5351.03 Supervising Cash Handling Activities
- POL-U5351.06 Accepting Cash
- POL-U5351.10 Maintaining Physical Control Over Cash
- POL-U5351.11 Transporting Cash
- POL-U5351.13 Accepting, Processing and Securing Bankcard Information
- POL-U5351.14 Accepting, Processing and Securing Payments through the Internet
- POL-U5352.02 Billing Student Accounts
- POL-U5352.03 Applying Credit to Students' and General Receivable Accounts
- POL-U5352.08 Collecting Accounts Owed to the University
- POL-U5352.09 Collecting Long Term Student Loans
- POL-U5400.08 Conducting Background Checks
- POL-U5400.05 University Resources
- POL-U5400.11 Verifying Employment Eligibility
- POL-U5950.19 Reporting Loss of University Funds or Property
- POL-U7100.01 Student Records Policy
- POL-U7100.02 Using Email for Official Correspondence with Students
- Ethical Conduct; WWU User Agreement for WWU Network and Computer Resources
- WWU Technology Security Incident Response Program
- Data Security, Passwords, and WWU Computer Use
- Maintaining Privacy and Security and University Computers
- Password Aging for All University Accounts

#### 4. Security Program Components

The Gramm-Leach-Bliley Act (GLBA), requires the University to:

- a) Designate an employee or employees to coordinate the information security program;
- b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of covered data that could result in the unauthorized disclosure, misuse or alteration, and assess the safeguards in place to control these risks;
- c) Design and implement covered data physical and electronic safeguards to control the risks the University identifies through risk assessment and regularly test and monitor the effectiveness of the safeguards' controls and procedures;
- d) Oversee service providers by selecting and retaining service providers who are capable of maintaining appropriate safeguards for university covered data; and
- e) Evaluate and adjust the program in light of relevant circumstances, including changes in technology or the results of testing and monitoring of safeguards.

## 5. Security Program Coordinator

The Vice President of Financial Affairs appoints the Internal Control Officer to serve as the Information Security Program Coordinator. The coordinator will work closely with the relevant academic and administrative departments throughout the university to accomplish security program components noted above.

## 6. Security Risk Assessment

The Non-Public Financial Information Security Program Coordinator must work with relevant offices of the University to identify reasonable foreseeable internal and external risks to the security, confidentiality, and integrity of covered data; assess the adequacy of safeguards in place to control the risks; design and implement physical safeguards to control risks; and regularly test and/or monitor the effectiveness of the safeguards' controls and procedures.

These risks include, but are not limited to:

- a) Unauthorized access of covered data by someone other than the owner of the covered data;
- b) Compromised system security as a result of system access by an unauthorized person;
- c) Interception of data during transmission;
- d) Loss of data integrity;
- e) Physical loss of data in a disaster;
- f) Errors introduced into the system;
- g) Corruption of data or systems;
- h) Unauthorized access of covered data by employees;
- i) Unauthorized requests for covered data;
- j) Unauthorized access through hardcopy files or reports; and
- k) Unauthorized transfer of covered data through third parties.

Risk assessment includes consideration of employee training and management, information systems, and information processing, storage, transmission and disposal. Risk assessment also considers systems for detecting, preventing, and responding to attacks, intrusions, or other external and internal risks to the security, confidentiality, and integrity of covered data. All elements noted could result in the unauthorized disclosure, misuse, alteration, destruction, or otherwise compromise of covered data. A risk assessment nevertheless will assess the adequacy of the safeguards in place to control these risks.

The Program Coordinator will utilize the *GLBA Risk Assessment/Internal Controls Matrix* as a tool to identify and assess the risks to information security. This assessment identifies the risks associated with unauthorized access to or transfer of covered data and the university wide controls that are currently in place to control the risks. The assessment will also be used to report the department-specific risks, and support the content of the Information Security Program Annual Report.

## 7. Information Safeguards and Monitoring

The *GLBA Risk Assessment/Internal Controls Matrix* will incorporate specific safeguard elements incorporated at the University:

- a) Employee Managing and Training

Safeguarding methods will include training of those individuals with authorized access to covered data. Upon identification of the employees who have access to covered data, the Coordinator will ensure that training is provided and necessitate:

- I. Proper use of computer covered data and passwords;
- II. The importance of confidentiality of student records, student financial information, and other types of covered data;
- III. Procedures to prevent employees from providing confidential information to an unauthorized individual;
- IV. Proper disposition (shredding) of documents that contain covered data; and
- V. Prompt reporting of identity theft to appropriate administration.

#### b) Physical Security

Each university department that is responsible for maintaining covered data must secure the information in accordance with the WWU Code of Responsibility for Security and Confidentiality of Records and Files and Student Records Policy, to protect it from destruction, loss or damage due to environmental hazards, or technical failures. The Program Coordinator will evaluate departmental physical security as part of the GLBA Risk/Assessment. The evaluation will identify:

- I. Access to covered data is limited to those employees who have employment specific reason to gain access to such information
- II. All university covered accounts including loan applications and Free Application for Federal Student Aid - FAFSA will be kept in locked file cabinets, rooms, or vaults that are required to be locked each night.
- III. Paper documents containing covered data will be shredded in a timely manner

#### c) Computing System Security and Safeguard Failures

The WWU Academic Technology and User Services (ATUS) is responsible for maintaining systems to prevent, detect, and respond to attacks, intrusions, and other system failures. The Program Coordinator will evaluate network access and security policies and protocols for responding to network attacks

and intrusions. Any security breaches or other system failures must be reported to the Chief Information Officer. The Chief Information Officer will notify the Security Incident Response Team to review and designate action where necessary. The Program Coordinator who is a member of the Security Incident Team will notify the Information Security Program Oversight Committee of the security breach and action to be taken.

#### d) Monitoring and Testing

The Program Coordinator will monitor the Non-Public Financial Information Security Program and periodically assess the current safeguards and make recommendations for safeguards. Based on these assessments, the Program Coordinator will work with all appropriate individuals to implement, correct, design, or improve safeguards.

### 8. Service Providers

In the course of business, the University may appropriately share covered data with third parties. Such activity may include collection activities, transmission of documents, transfer of funds, destruction of documents, or other similar services. The Information Security Program will ensure that the selection process for third party service providers include an evaluation of the ability for the service provider to safeguard confidential University covered data. University decisions to select and retain service providers will be based on the capability of service providers to develop and maintain appropriate safeguards for covered data at issue, and require service providers by contract to implement and maintain such safeguards.

Contracts with service providers that will maintain or regularly access covered data shall include, but not be limited to, the following provisions:

- a) An explicit acknowledgement that the contract allows the contract partner access to covered data;
- b) A specific definition or description of the covered data being provided;
- c) A stipulation that the covered data will be held in strict confidence and accessed only for the explicit business purpose of the contract;
- d) An assurance from the contract partner that the partner will protect the covered data;

- e) A provision providing for the return or destruction of all covered data received by the contract provider upon completion or termination of the contract;
- f) An agreement that any violation of the contract's confidentiality conditions may constitute a material breach of the contract and entitles WWU to terminate the contract without penalty; and
- g) A provision ensuring that the contract's confidentiality requirements shall survive any termination agreement

## 9. Continuing Evaluation and Adjustment

Continued administration of the development, implementation and maintenance of WWU's Information Security Program is the responsibility of the Information Security Program Coordinator. The Program Coordinator, in conjunction with the Program Plan Oversight Committee, will periodically meet to discuss adjustments to the Program to reflect changes in technology, the sensitivity of covered data, and internal and external threats to the security of covered data.

The Internal Audit Department may conduct periodic reviews of areas that have access to covered data to assess the internal control environment established by the administration and to verify the WWU departments comply with the requirements of Policy POL-U5300.01 Safeguarding Non-Public Financial Information and the Information Security Program.