

POLICY

Effective Date: May 22, 2006

Approved By: President's Council

See Also:

WWU Information Security Program Plan

Administrative Computing Services – Security Plan for Information Technology

Family Educational Rights and Privacy Act (FERPA)

Gramm-Leach-Bliley Act (GLBA)

RCW 42.56.590

University Records – Definition and Management Policy

POL-U5950.19; PRO-U5950.19A Reporting Loss of University Funds

POL-U5300.01 SAFEGUARDING NON-PUBLIC FINANCIAL INFORMATION

This policy applies to all university employees who are responsible for, have access to, or handle student records and other non-public, financial information.

Definitions:

Covered data

Covered data for the purpose of this policy includes, but is not limited to, student financial information (defined below) required to be protected under the Gramm-Leach-Bliley Act (GLBA). Covered data includes both paper and electronic records.

Covered data does not explicitly include checks, credit card, and debit card information handled in areas of the University in the course of business, such as the A.S. Bookstore. However, the university recognizes that this information is confidential, and will provide focused safeguards training in these areas.

Student financial information

Student financial information consists of information that Western Washington University has obtained from a student, parent, other postsecondary institution, lending institution, guarantee agency, the U.S. Department of Education, scholarship donors and others in the process of offering a financial product or service. Offering a financial product or service includes offering student grants, loans, need-based employment or scholarships to students, receiving income tax information from a student and/or the student's parent, reporting calculated student need for federal, state and local agencies, and any other miscellaneous financial service. Student financial information includes addresses, phone numbers, bank, debit, and credit card account numbers, income and credit histories and Social Security numbers, in both

POLICY

paper and electronic format, if the information has been obtained in the course of offering a financial product or service.

Service Providers

Service providers refer to all third parties who, in the ordinary course of university business, are provided access to covered data. Service providers may include, but are not limited to, businesses retained to transport and dispose of covered data, collection agencies, loan processing agencies, and systems support providers.

1. The University Maintains a Financial Information Security Program

- A. The purpose of the university's Financial Information Security Program is to maintain safeguards to protect covered data by:
 - i. Ensuring the security and confidentiality of covered data;
 - ii. Protecting against anticipated threats or hazards to the security or integrity of such information; and
 - iii. Protecting against unauthorized access to or use of covered data that could result in substantial harm or inconvenience to any customer.
- B. The Financial Information Security Program provides mechanisms to:
 - i. Identify and assess the risks that may threaten covered data maintained by WWU;
 - ii. Develop written policies and procedures to manage and control these risks;
 - iii. Implement and review the plan; and
 - iv. Adjust the plan to reflect changes in technology, the sensitivity of covered data and information and internal or external threats to information security.
- C. WWU's Financial Information Security Program will incorporate, but not be limited to, information security safeguards in the following areas:
 - i. Employee management and training
 - ii. Physical security
 - iii. Computing system security
 - iv. Security safeguard failures
 - v. Selecting appropriate Service Providers

POLICY

2. **The Vice President of Business and Financial Affairs Appoints the University's Financial Information Security Program Coordinator and Authorizes Program Activities**

The Vice President of Business and Financial Affairs appoints the university's Financial Information Security Program Coordinator and authorizes the activities necessary for the Coordinator to implement and maintain the program.

3. **The Vice President of Business and Financial Affairs Appoints the University's Financial Information Security Program Oversight Committee**

The Vice President of Business and Financial Affairs will appoint managers from relevant university departments to serve on the Oversight Committee. These departments may include, but are not limited to, Financial Aid, Registrar, Administrative Computing Services, and Internal Audit.

4. **Financial Information Security Program Oversight Committee Reviews Program Activities**

The purpose of the Financial Information Security Program Oversight Committee is to provide a high level review of program activities.

The Oversight Committee will meet with the Coordinator at least annually.

5. **The University Periodically Reviews and Adjusts the Financial Information Security Program**

The Coordinator, in conjunction with the Oversight Committee, will periodically review and adjust the Security Program to reflect changes in technology, changes in law, the sensitivity of student/customer data, and internal or external threats to information security.

Internal Audit personnel may conduct periodic reviews to areas that have access to covered data to assess the internal control structure put in place by the administration and to verify that WWU departments comply with the requirements of this policy and the Financial Information Security Program.