

# INFORMATION SECURITY PLAN FOR CASE WESTERN RESERVE UNIVERSITY

## I. INTRODUCTION

As part of its educational mission, Case Western Reserve University ("CWRU") acquires, develops, and maintains data and information, computers, computer systems and networks. These information technology resources are intended for CWRU-related purposes, including direct and indirect support of CWRU's educational, research and service missions; CWRU's administrative functions; student and campus life activities; and the free exchange of ideas with CWRU's community and among the wider, local, national and world communities. In order to protect the information which is acquired, developed and maintained by CWRU and to comply with Federal Law, specifically The Financial Services Modernization Act of 1999 (also known as Gramm Leach Bliley Act ("GLBA"), 15 U.S.C. § 6801, CWRU will have an Information Security Plan ("Plan").<sup>1</sup>

## II. THE GRAMM LEACH BLILEY ACT REQUIREMENTS

The GLBA requires that CWRU appoint an Information Security Plan Coordinator to assess the risk of likely security breaches, institute a training program for all employees who have access to covered data and information, oversee service providers and contracts and evaluate and adjust the Plan periodically.

## III. THE COORDINATOR

In order to comply with GLBA, CWRU has designated the Chief Information Officer ("CIO") to coordinate the Plan. All correspondence and inquiries with regard to the Plan should be directed to the CIO.

The CIO will assist affected Schools and Departments in identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information which could result in the compromise of such information. The CIO will also evaluate the effectiveness of the current safeguards for controlling these risks; design and implement a safeguards program; and regularly monitor and evaluate the program.

---

<sup>1</sup>For the purposes of this Plan, **covered data and information** includes, but is not limited to, student financial information required to be protected under the GLB. **Student financial information** is that information which CWRU has obtained from a student in the process of offering a financial product or service, or such information provided to CWRU by another financial institution. Offering a financial product or service includes offering student loans to students, receiving tax information from a student's parent when offering a financial aid package, or other miscellaneous financial services as defined in 12 CFR § 225.28. Examples of student financial information includes addresses, telephone numbers, bank and credit card account numbers, income and credit histories, and social security numbers, in both paper and electronic format.

#### **IV. RELEVANT AREAS**

Relevant areas to be considered when assessing the risks to customer information include:

- Human Resources / Payroll
- Affected Information Systems / Information Technology Services
- Service Providers
- Student Loans
- Admissions
- Registrar's Office
- Financial Aid Office
- Bursar's Office / Accounts Receivable
- Residence Life
- Rental Property and Property Management
- Continuing Education
- Annuity Funds
- Management Centers

#### **V. COORDINATION OF CWRU'S INFORMATION SECURITY PLAN**

The CIO will implement and update the Plan and will coordinate with the Internal Auditor to test the Plan. The Registrar will provide guidance to the CIO concerning compliance with the Family Educational Rights and Privacy Act. Each relevant area is responsible to secure customer information in accordance with all privacy guidelines. A written security policy detailing the information security policies and processes will be maintained by each relevant area and will be made available to the CIO and/or the Internal Auditor upon request.

In addition, Information Technology Services will maintain and provide access to administrative procedures that protect against any anticipated threats to the security or integrity of electronic customer information and which guard against the unauthorized use of such information.

#### **VI. SERVICE PROVIDERS**

Service Providers that are given access to covered data and information will be neither selected nor retained unless they provide adequate safeguards. Contracts with service providers shall include the following provisions:

- a specific definition of the confidential information being provided;
- a stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract;
- a guarantee from the contract partner that it will ensure compliance with the protective conditions outlined in the contract;
- a guarantee from the contract partner that it will protect the confidential information it accesses according to commercially acceptable standards and no less rigorously than it protects its own customers' confidential information;
- a provision allowing for the return or destruction of all confidential information received by the contract partner upon completion of the contract;
- a stipulation allowing the entry of injunctive relief without posting bond in order to prevent or remedy breach of the confidentiality obligations of the contract;
- a stipulation that any violation of the contract's protective conditions amounts to a material breach of contract and entitles CWRU to immediately terminate the contract without penalty;
- a provision which requires the service provider to defend, indemnify, and hold CWRU harmless for any damages resulting from violation of the contract's protective conditions;
- a provision allowing auditing of the contract partners' compliance with the contract safeguard requirements; and
- a provision ensuring that the contract's protective requirements shall survive any termination of the agreement.

## **VII. EMPLOYEE TRAINING AND EDUCATION**

While directors and supervisors are ultimately responsible for ensuring compliance with information security practices, the CIO, in cooperation with the Office of Human Resources, will develop training and education programs for all employees who have access to covered data.

## **VIII. EVALUATION AND REVISION OF THE PLAN**

The Plan shall be evaluated and adjusted in light of relevant circumstances, including changes in CWRU's business arrangements or operation, or as a result of testing and monitoring the safeguards. Periodic auditing of each relevant area's compliance and general risk assessment will be performed as determined by the Internal Auditor. Evaluation of the risk of new or changed business arrangements will be done in consultation with the Office of the Vice President and General Counsel.