

**University of Southern California**  
**Policy and Procedures for the Protection of Consumer Financial Information**  
**Under the Gramm-Leach-Bliley Act**

Date Issued: April 7, 2004

Authority: Lloyd Armstrong, Jr.,  
Provost and Senior Vice President for Academic Affairs

Dennis F. Dougherty  
Senior Vice President for Administration

**1.0 Introduction**

The University of Southern California (USC) is committed to protecting the privacy of non-public customer information. The purpose of this policy is to describe the university's policies and procedures for complying with the specific requirements set forth in the federal Gramm-Leach-Bliley Act (GLB Act).

This policy describes how the university protects information specifically covered under the GLB Act. This document is a subset of the university's umbrella policy regarding information security, which identifies all information requiring special protections.

1.1 Summary of Requirements of GLB Act

The GLB Act requires "Financial Institutions," defined below, including universities, to protect non-public personal information that is collected from an individual who obtains or has obtained a financial product or service from the institution for personal, family or household purposes.

Financial products or services offered by USC and covered by the GLB Act include, but is not limited to:

- Student loans
- Faculty, staff and other employee loans
- USCard

Examples of information that would require protection include tax returns, Social Security numbers or other non-public or personal information that is collected for purposes of providing these services.

The safeguarding regulations of the GLB Act (“Safeguards Rule”) require that covered institutions, such as USC, develop, implement and maintain a comprehensive information security plan that includes administrative, technical and physical safeguards to protect the information covered by the GLB Act. The plan must describe how USC protects customer information.

## **2.0 Definitions**

### **2.1 Financial Institution**

An institution significantly engaged in financial activities, which include:

- lending, exchanging, transferring, investing for others, or safeguarding money or securities. These activities cover services offered by lenders, check cashers, wire transfer services, and sellers of money orders.
- providing financial, investment or economic advisory services. These activities cover services offered by credit counselors, financial planners, tax preparers, accountants, and investment advisors.
- brokering loans.
- servicing loans.
- debt collecting.
- providing real estate settlement services.
- career counseling (of individuals seeking employment in the financial services industry).

### **2.2. Financial Product or Service**

A financial product or service covered under the GLB Act includes the following:

- offering student, faculty or staff loans;
- making, acquiring, brokering, or servicing loans or other extensions of credit;
- real estate and personal property appraising;
- arranging commercial real estate equity financing;
- collection agency services; and
- credit bureau services.

### **2.3 Consumer**

Someone who obtains or has obtained a financial produce or service from a financial institution that is to be used primarily for personal, family or household purposes, or that person’s legal representative. Examples include:

---

Issued by: Lloyd Armstrong, Jr.  
Provost and Senior Vice President, Academic Affairs  
Dennis F. Dougherty  
Senior Vice President for Administration

Date issued: April 7, 2004

- making a wire transfer; or
- applying for a loan, whether or not the individual actually obtains the loan.

#### 2.4 Customer

Customers are consumers who have a continuing relationship with a financial institution. Examples include:

- opening a credit card account with a financial institutions; or
- using the services of a mortgage broker to secure financing.

#### 2.5 Non-Public Personal Information

Any personal identifiable financial information that a financial institution collects about an individual in connection with providing a financial product or service, unless that information is otherwise publicly available. Examples include:

- any information an individual gives to get a financial product or service (for example, name, address, income, Social Security number, or other information on an application);
- any information received about an individual from a transaction involving an institution's financial product(s) or service(s) (for example, the fact that an individual is a consumer or customer, account numbers, payment history, loan or deposit balances, and credit or debit card purchases); or
- any information received about an individual in connection with providing a financial product or service (for example, information from court records or from a consumer report).

### 3.0 Policy

The University shall comply with the Safeguards Rule, which requires the institution to:

- Designate one or more employees to coordinate the program;
- Identify “reasonably foreseeable” internal and external risks to the security and confidentiality of customer information that could lead to unauthorized disclosure, use, alteration, destruction or other compromise of such information and “assess the sufficiency” of the institution’s safeguards in place to control these risks. Such risk assessment must include, at a minimum, risks in areas of operation such as:

---

Issued by: Lloyd Armstrong, Jr.  
Provost and Senior Vice President, Academic Affairs  
Dennis F. Dougherty  
Senior Vice President for Administration

Date issued: April 7, 2004

- Employee training and management,
  - information systems, and
  - detecting, preventing, and responding to attacks against the institution's systems;
- Implement safeguards to manage the identified risks and regularly test or monitor such safeguards;
- Oversee the institution's service providers by:
  - Selecting and retaining service providers that are capable of maintaining appropriate safeguards for the customer information at issue, and
  - Requiring service providers by contract to implement and maintain such safeguards; and
- Evaluate and adjust the institution's security program in light of such risk assessment, any material change to institutional business operations or any other circumstances that may have a material impact on the institution's information security program.

Section 4.0 of this document describes the procedures for implementing the above policy.

#### **4.0 Procedures**

##### 4.1 Employee Designation

USC's Information Security Officer is responsible for day-to-day management and oversight of the university's information security plan, including the Safeguards Rule of the GLB Act. The following offices will specifically assist in protecting data covered by the GLB Act:

- Dean of Academic Records and Registrar
- Assistant Vice President, Administrative Information Systems (Bursars systems)
- Director, Space and Equipment Management, Student Financial Services
- Associate Dean/Director, Financial Aid
- Associate Treasurer, Office of the Treasurer
- Director, Student Information Systems
- Director, USCard Services

##### 4.2 Risk Assessment

---

Issued by: Lloyd Armstrong, Jr.  
 Provost and Senior Vice President, Academic Affairs  
 Dennis F. Dougherty  
 Senior Vice President for Administration

Date issued: April 7, 2004

Page 4 of 7

USC units that may be impacted by the Safeguards Rule of the GLB Act include, but are not limited to:

- Financial Aid,
- Registrar's office,
- Student Financial Services,
- USCard,
- Treasurer's office (for processing staff and faculty housing loans), and
- Student Information Systems (SIS), which maintains student information covered under the GLB Act.

Each of these units continues to implement security procedures to comply with the GLB Act. The Information Security Officer coordinates with these units to assist with compliance under the GLB Act.

The Office of Audit Services will assist in these efforts by conducting risk assessments for the university in the area of information security.

#### 4.3 Training

As of 2002, all university staff employees who have access to customer information undergo a background check prior to hire, pursuant to university policy.

All individuals who access student education records must complete a training program regarding the Family Educational Rights and Privacy Act (FERPA) before they are provided access to systems that maintain this information. All users of the Student Information Systems (SIS) must sign User Agreements, acknowledging their respective responsibilities to maintain the confidentiality of student information.

Additional employee training and awareness campaigns, as well as analysis of university information systems and incident reporting procedures are addressed in the university wide information security program. The requirements of the Safeguards Rule are incorporated into the university information security program.

#### 4.4. Incident Reporting

All incidents of actual or suspected security breaches must be reported immediately to the appropriate individual listed above in Section 4.1 as well as the Information Security Office of the Office of Compliance at (213) 743-4900 or infosec@usc.edu.

---

Issued by: Lloyd Armstrong, Jr.  
Provost and Senior Vice President, Academic Affairs  
Dennis F. Dougherty  
Senior Vice President for Administration

Date issued: April 7, 2004

#### 4.5 Implementing Safeguards

The university already has several formal policies and procedures that address information security of the data covered by the GLB Act as well as consequences for failing to maintain the confidentiality of certain information, including:

- Family Educational Rights and Privacy Act (FERPA) policy,
- Personal Information Policy,
- USC Misappropriation of Assets,
- Student Conduct Code,
- Faculty Handbook,
- Staff Employment Policies and Procedures, and
- Information Services Division Acceptable Use Procedures.

These policies and procedures can be found at [www.usc.edu/policies](http://www.usc.edu/policies).

The university also has implemented certain procedures to restrict access to certain student information, including information protected under the GLB Act, including:

- SIS User Agreement (described above),
- Automatic termination of access to SIS upon employee termination or resignation, and
- Access control restrictions depending upon employee roles and responsibilities.

The university's information security program incorporates the following safeguards, as appropriate:

- Locking rooms and file cabinets where paper records are kept,
- Ensure that storage areas are protected against destruction or potential damage from physical hazards,
- Using password-activated screensavers,
- Using strong passwords,
- Storing electronic customer information on a secure server,
- Maintain secure backup media and keep archived data secure,
- Changing passwords periodically,
- Encrypting customer information when it is transmitted electronically over networks or stored online, when possible,
- Referring calls or other requests for customer information to designated individuals who have had appropriate training for addressing such requests,
- Reporting incidents of fraudulent or suspicious attempts to obtain customer information,

---

Issued by: Lloyd Armstrong, Jr.  
Provost and Senior Vice President, Academic Affairs  
Dennis F. Dougherty  
Senior Vice President for Administration

Date issued: April 7, 2004

- Disposing of customer information in a secure manner, such as shredding or erasing data when disposing of computers and recycling,
- Including confidentiality provisions in the university's standard offer letters, and
- Including confidentiality provisions in the university's standard purchase order and independent contractor agreements.

#### 4.6 Oversight of Service Providers

The University takes reasonable and appropriate steps to select and retain providers that comply with the privacy and security regulations and requirements. Service providers are contractually obligated to comply with applicable privacy and security laws and regulations.

The University's standard purchase order and independent contractor agreements with vendors include appropriate confidentiality provisions in this regard.

#### 4.7 Monitoring and Auditing

Compliance with the GLB Safeguards Rule shall be monitored regularly in conjunction with the university's monitoring of its information security program. Audit Services will conduct periodic internal audits to ensure compliance with federal and state laws and regulations as well as university policy.

### 5.0 Resources

Federal Trade Commission:

<http://www.ftc.gov/privacy/privacyinitiatives/safeguards.html>

U.S. Senate Committee on Banking, Housing and Urban Affairs: Information Regarding the Gramm-Leach-Bliley Act of 1999

<http://www.senate.gov/~banking/conf/>

National Association of College and University Business Officers: 2003-01 Colleges and Universities Subject to New FTC Rules Safeguarding Customer Information (January 13, 2003)

[http://www.nacubo.org/nacubo\\_reports/](http://www.nacubo.org/nacubo_reports/)