I. SUMMARY

This guideline is designed to promote University compliance with the Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act), and specifically with the GLB Safeguarding Rule issued by the Federal Trade Commission. This applies to safeguarding customer information for loans to students, parents, and employees. It may apply to other financial transactions involving customer information.

UC entities and processes (whether or not they handle customer information, as defined by the Federal Trade Commission in Federal Register 16 CFR Part 313.3) are bound by current UC policies that govern information practices and security, including the Business & Finance (B&F) Bulletins for records management and privacy and for information systems.

Further, the University complies with applicable state and federal laws pertaining to information security and privacy, including the California Information Practices Act (IPA) for the protection of personal information generally, the Family Educational Rights and Privacy Act (FERPA) for the protection of information contained in student records, and the Health Insurance Portability and Accountability Act (HIPAA) for the management of patients’ personal and health information.

II. DEFINITIONS

Customer Information: The GLB Compliance Plan uses the term “customer information” as defined in the GLB Safeguarding Rule, 16 CFR 314.2 (incorporating other definitions from the GLB Privacy Rule, 16 CFR 313.3). Relevant definitions are included in Exhibit A. For purposes of this plan, customer information at UC includes the following data elements, whether stored as paper records or electronically:

- Name
- Home address
- Home phone number
- Name of spouse or other relatives
- Citizenship
- Bank and credit card number
- Income and credit histories
III. GUIDANCE TEXT

A. UC GLB Compliance Plan

The University of California seeks to ensure that appropriate measures are implemented to protect the privacy of individuals’ personal information, and to broadly educate the University community not only about state and federal laws governing information management and security, but also about the responsibility of all employees to protect sensitive information.

The University’s written procedures for complying with the GLB Safeguarding Rule are available in several readily accessible parts:

- **Electronic Information Security Bulletin.** The protection of electronic personal information at UC is guided by systemwide policy, as detailed in Business and Finance Bulletins, IS-3 “Electronic Information Security.” Recognizing that UC customer information is now regularly if not solely found in electronic form, University compliance with GLB is principally guided by IS-3.

- **GLB Compliance Plan.** This GLB Compliance Plan provides specific direction for functional areas that fall under the purview of the GLB Safeguarding Rule.
  - It identifies the types of information that are subject to the GLB Safeguarding Rule.
  - It directs that all electronic information should be handled in accordance with the University’s comprehensive policy for protection of electronic information, Business and Finance Bulletins, IS-3 “Electronic Information Security.”
  - It clarifies expectations for the handling of paper records subject to the Rule, and which are not covered in IS-3.

- **Management Guide.** Additional practical guidance is provided in the Management Guide for Information Security at UC (IS-3).

- **Systemwide Websites.** Information and resources pertinent to safeguarding information are available at the systemwide information security web site.

- **Local Campus Websites.** Location-specific procedures and guidance are provided on campus and UCOP Web sites devoted to information security. These may be found listed on the systemwide information security web site.

B. Overview of Compliance Plan Requirements

**Protection of Electronic Customer Information.** The comprehensive systemwide policy for protecting electronic information is Business and Finance bulletin IS-3, “Electronic Information Security.” Any UC organization that handles GLB customer information, as defined in this document, in electronic format must follow IS-3 procedures to protect that data in accordance with the GLB Safeguarding Rule. IS-3
fully addresses the GLB requirements for administrative, technical, and physical safeguards; risk assessment; employee training; and selection of and contracting with service providers with respect to electronic information. To avoid redundancy and confusion about precedence, this GLB Compliance Plan purposefully does not duplicate IS-3 provisions but expands upon them where necessary to ensure the University’s full compliance under the GLB Safeguarding Rule.

**Protection of Customer Information in Paper Records.** The Electronic Information Security policy, IS-3, does not address paper records at this time. Therefore, specific guidance for ensuring that the University protects paper records containing customer information covered under the GLB is provided in the following pages. In summary, University units that handle GLB customer information must address the handling of paper records, especially with respect to:

- risk assessment and subsequent implementation of safeguards,
- employee training and management,
- selection of and contracts with service providers, as well as testing, monitoring, and evaluation of safeguards, and;
- for both electronic and paper records—overall evaluation of the information security program and its effectiveness in protecting GLB customer information.

**C. UC GLB Compliance Plan Coordinator**

The Vice President for Information Technology Services (VP-ITS) based at the UC Office of the President (UCOP) serves as the GLB Compliance Plan Coordinator for the UC system. In this capacity, the VP-ITS coordinates implementation of the program with campus individuals who by policy have been conferred authority for financial management, as well as information security and records management. These include the Controllers, the Coordinators of Information Practices, Information Security Coordinators, and lead campus authorities for ensuring notification to affected individuals in the event of security breaches.

The Coordinator ensures that applicable entities are notified of their responsibilities to implement IS-3 for all electronic customer information and to develop procedures to protect paper records in accordance with the GLB Compliance Plan.

**D. Scope of Applicability of the UC GLB Compliance Plan**

The UC GLB Compliance Plan shall be implemented by all organizations or entities governed by the Regents of the University of California. It also shall be implemented by the UC-managed national laboratories for the purpose of safeguarding "unclassified" personal information; existing safeguards for classified information provide appropriate compliance with the GLB Safeguarding Rule.

The types of financial services or products that are subject to the GLB Safeguarding Rule are identified in the chart below. Functional areas that handle the financial services or products, or the customer information pertaining to them, during the course of their operations must comply with the GLB Compliance Plan and ensure
Appropriate safeguarding of the customer information.

<table>
<thead>
<tr>
<th>Financial Services or Products Covered by the GLB Safeguarding Rule</th>
<th>Examples of Functional Areas that May Handle these Services or Products</th>
</tr>
</thead>
</table>
| ► Student loans (bank loans, federal loans, UC loans)            | ► Financial Aid  
| ► Emergency student loans (undergraduate and graduate)          | ► Student Accounts Receivable  
| ► Parent loans                                                  | ► Student Loan Administration  
| ► Repayable scholarships                                       | ► Billing  
|                                                                  | ► Business Services  
|                                                                  | ► Bursar’s Office |
| ► 403(b) loans                                                  | ► Human Resources  
|                                                                  | ► Benefits |
| ► Emergency faculty loans                                      | ► Billing  
| ► Emergency staff loans                                        | ► Business Services  
|                                                                  | ► Loans and Receivables |
| ► Faculty and staff home loans                                  | ► Office of Loan Programs  
|                                                                  | ► Payroll |

In general, the Safeguarding Rule covers activities that banks by regulation are authorized to engage in. At UC, this translates principally to loans to students, parents, and employees.

Types of financial transactions that do not meet the technical definition of a “financial service or product,” and/or do not result in a “customer relationship” as defined under the GLB Safeguarding Rule are listed below:

**Monetary gifts or payments requiring no repayment:** grants, scholarships, and fellowships; fee remissions; traineeships; work study; payroll; monthly pension payments; one-time pension disbursements

**Lease agreements:** rental or housing agreements

**Retail or “layaway” types of transactions:** deferred payment plans for fees and non-resident tuition; payment plans for student debts; campus debit cards; payment plans for medical services

**Types of insurance that banks are not authorized to issue:** student and employee health insurance; life insurance

**Processes for transferring funds unrelated to covered financial products or services:** billing services for amounts owed by students, staff, faculty, and outside vendors; issuance of checks or electronic funds transfer (EFT) payments to students.
E. **Risk Assessment and Implementation of Safeguards**

Departments that handle information subject to the GLB Safeguarding Rule must conduct periodic risk assessments and should ensure the assessments cover both paper records and electronic records.

Guidance about conducting risk assessments is available in IS-3.

The purpose of the risk assessment is to identify reasonably foreseeable internal and external risks to security, to assess the sufficiency of safeguards in place to control these risks, and to design and implement new or revised safeguards to control identified risks.

**Risk Assessment.** The risk assessments will include an analysis of the various risks and effectiveness of management practices currently in place to ensure compliance and security enhancement. Risk assessments must involve a consideration of risks in each relevant area of operations and cover processes for handling, storing, and disposing of the paper records; processes for detecting, preventing, and responding to security failures; and employee training and management, including the appropriateness and frequency of staff and management security awareness training.

**Design and Implementation of Safeguards.** As a result of the risk assessment, recommendations are made as necessary to change management practices to improve business controls and/or to implement information safeguards.

**Testing and Monitoring.** Regular testing and monitoring of the safeguards implemented as a result of the risk assessment will be conducted on a periodic basis.

**IS-3 Reference.** III B, Risk Assessment, Asset Inventory and Classification

F. **Employee Training and Management**

Based on the results of risk assessments, departments shall develop appropriate training programs to ensure staff is aware of protocols for protecting customer information. Any training program or materials should incorporate concepts relevant to both electronic and paper-based customer information, building on security training concepts in IS-3.

Department managers and supervisors are charged with keeping employees informed about policies and programs that pertain to their work, including those that govern information security and privacy. Managers and supervisors should ascertain which positions deal with customer information and assess whether these should be deemed “critical positions” requiring background checks, as provided for by UC personnel policy.

Department managers and supervisors are charged with ensuring employees complete UC’s mandatory security awareness training as assigned.

**IS-3 Reference.** III E, Education and Security Awareness Training
G. Selection of Service Providers

Current University policies that govern agreements with third-party service providers require that these service providers adhere to applicable state and federal laws and define requirements for the handling of confidential information, including both the safeguarding of customer information, as required by the GLB Safeguarding Rule, and notification to individuals if their unencrypted electronic personal information has been acquired by an unauthorized person through a security breach, as required by California Civil Code Section 1798.29.

Selection of Vendors. University departments seeking to contract with third parties to handle customer information will exercise due diligence to ensure that the vendor is capable of maintaining appropriate safeguards for the information, in keeping with Business and Finance Bulletin 43, Materiel Management.

Contract Language. All service contracts in which paper or electronic records containing the customer information protected by the GLB Safeguarding Rule must contain language to require, as necessary, the "safeguarding" of the University’s customer information and notification in instances of security breaches. Sample language developed by the Office of the General Counsel for use in contracts is available online as the UC Appendix – Data Security and Privacy (Appendix DS) which applies to both electronic and paper data.

IS-3 Reference: III F, Third-party Agreements

Resources on Agreements and Contracts: Procurement Services

H. Program Evaluation

This section covers both electronic and paper records, expanding on requirements in IS-3 for electronic information to ensure that an appropriate evaluation of compliance with the GLB Safeguarding Rule is conducted periodically.

Under this Plan, units are responsible for the routine testing, monitoring, and evaluation of safeguards implemented in the functional areas to minimize identified risks. This is accomplished primarily through routine self-assessments by departments and the University’s scheduled internal audits.

Controllers are responsible for ensuring that units periodically conduct testing and monitoring of safeguards, and program evaluation.

The University’s Internal Audit Program conducts independent audits and consultations in order to evaluate and promote the University’s system of internal controls. Currently, the Internal Audit Program periodically audits the business functional areas such as cash management, accounts payable, financial aid, fund raising and gift processing, student fees and receivables, disbursements, and medical billing and receivables. These functional areas overlap with areas identified for compliance with the GLB Compliance Plan. Internal audits incorporate an evaluation of implementation of the GLB Compliance Plan and IS-3 since standard
audits review compliance with policy, adequacy of risk controls, management information flow, and business effectiveness and efficiency.

All employees by policy have access to “whistleblower” provisions if they believe serious violations of University policy or law are occurring. The whistleblower provision could apply if an employee believed that customer and personal information were willfully not being protected and that such concerns were not being properly considered by the personnel in authority.


IV. COMPLIANCE/RESPONSIBILITIES

The Vice President for Information Technology Services serves as the GLB Compliance Plan Coordinator, and is responsible for systemwide compliance with the GLB Safeguarding Rule through appropriate communication with and coordination among applicable groups.

Managers of functional areas that must comply with the GLB Safeguarding Rule are responsible for setting in place the processes by which their unit personnel comply with Business and Finance Bulletin IS-3, “Electronic Security Information,” and for incorporating into the unit’s IS-3 information security program specific plans and procedures for protecting customer information found in paper records.

Managers and supervisors are responsible for ensuring that employees (a) are aware of and understand how to implement their unit’s information security program and other applicable policies and programs and (b) are appropriately trained in compliance, including detecting, handling, and reporting security breach incidents.

Campus controllers assist units with setting risk evaluation schedules and processes as requested.

University auditors are responsible for reviewing conformance to the GLB Compliance Plan as part of routine internal audits.

Electronic systems personnel are responsible for complying with IS-3.

All University employees are responsible for conducting their work in accordance with University policies and procedures, for reporting concerns to their supervisor or, if necessary, through the Whistleblower Policy.

V. RELATED INFORMATION

**Personnel Policies for Staff Members (PPSM) 21: Selection and Appointment:**
- Requires job-related background information on final candidates for critical positions and employees who are promoted, reclassified, or transferred into critical positions.

**Policies applying to the Disclosure of Information from Student Records—130.00:**
- Interprets the application of the Family Educational Rights and Privacy Act (FERPA): “Student records include, but are not limited to, academic evaluations, including student examination papers, transcripts, test scores and other
academic records; general counseling and advising records; disciplinary records; and financial aid records, including student loan collection records." In this policy, the term "personally identifiable information" means "any information that identifies or describes a student. It includes, but is not limited to, a student's name, the name of a student's parent or other family members, the address of a student or student's family, any personal identifier such as a student's social security number, and any personal characteristics or other information that would make a student's identity easily traceable."

University of California Policy on Reporting and Investigating Allegations of Suspected Improper Governmental Activities (Whistleblower Policy)

- Encourages employees to use guidance provided by the policy for reporting all allegations of suspected improper governmental activities. The policy states that the University has a responsibility for the stewardship of University resources, which includes University records.

Business and Finance (B&F) Bulletins

B&F Bulletin IS-2, “Inventory, Classification, and Release of University Electronic Information”

- Establishes guidelines for the classification of information assets to aid risk assessments and to identify the need for specific security measures.

- Distinguishes between confidential, personal and public, and restricted data. Restricted information is any confidential or personal information that is protected by law or policy and that requires the highest level of security.


- Defines “personal” computerized information for which notification must be made about any breach of security (B&F Bulletin IS-3, section III.D, “Notification in Instances of Security Breaches Involving Personal Information Data”).

- Requires campuses to identify an information security officer and establish an information security program.

- Requires a risk assessment that includes an inventory of all information resources and requires development of an information security plan, based on the risk assessment that identifies “the level of security necessary for the protection of resources” along with administrative, technical, and physical safeguards for implementation.

- Establishes that the risk assessment must cover staff and management training. Further specifies that security awareness training should be conducted routinely.

- Specifies that agreements with third-party vendors or business associates should include “satisfactory assurances that the contracting third party will appropriately safeguard information.”

- Requires that the Information Security Officer be responsible for “periodic evaluation of the Program to ensure that the Program adequately addresses operational or environmental changes.”

B&F Bulletin IS-12, “Continuity Planning and Disaster Recovery”
• Provides recommendations and guidelines for information technology continuity planning and disaster recovery activities in support of the University’s commitment to protection of and accessibility to information resources.

• States that risk assessments should identify the availability requirements of resources according to their criticality and priority status, and that all resources should be classified as essential, necessary, or deferrable.


• Establishes responsibilities for privacy of and access to all information maintained by any segment of the University, except for those records pertaining to students.

B&F Bulletin RMP-12, “Guidelines for Assuring Privacy of Personal Information in Mailing Lists and Telephone Directories”

• Establishes privacy guidelines with respect to mailing lists and telephone directories.

B&F Bulletin BUS-34, “Securing the Services of Independent Consultants:”

• Securing the Services of Independent Consultants,” Exhibit A, is the required form for an Independent Consultant Agreement. Section XII of the form, Records about Individuals, states that the California Information Practices Act and University policies establish “certain requirements and safeguards regarding records pertaining to individuals, including the rights of access by the subject individual and by third parties.” Section XII specifies how the consultant shall treat confidential or personal records about individuals.

Exhibit A, section XIII, “Ownership and Access to Records,” says that ownership of records with confidential or personal information are subject to negotiation but will “normally become the property of UC and subject to state law and university policy governing privacy and access to files.”

Exhibit A, section XVII, “Confidentiality,” establishes a nondisclosure provision: “The Consultant shall use his or her best efforts to keep confidential any information provided by the University and marked ‘Confidential Information,’ or any oral information conveyed to the Consultant by the University and followed by a written communication within thirty (30) days that said information shall be considered Confidential Information.”

B&F Bulletin BUS 43, Materiel Management:

• Related to Purchase Transactions – Materiel Managers:

  o Shall determine bidders are responsible. A responsible bidder has the capability in all respects to fully perform the contract requirements and whose integrity and reliability will assure good faith performance.

  o Shall reject bids where that are non-responsive, or that are from a bidder who is not responsible.

• References the UC Terms and Conditions of Purchase which requires:

  o Supplier to agrees to procure all necessary permits or licenses and abide
by all applicable laws, regulations and ordinances of the United States and of the state, territory and political subdivision or any other country in which the Services are provided.

- Any provision required to be included in a contract of this type by any applicable and valid federal, state or local law, ordinance, rule or regulations will be deemed to be incorporated herein.

- The law of the State of California shall control the UC Terms and Conditions of Purchase and any document to which it is appended.

VI. REVISION HISTORY

**August 28, 2017:** This guideline was remediated to meet Web Content Accessibility Guidelines (WCAG) 2.0.

**February 6, 2017:** Technical update. Fixed/removed changed hyperlinks. Removed references to RMP-8 – this policy was rescinded and issued as a guideline. Added revision history and page numbers.

**May 7, 2012:** The plan was reformatted into the standard University of California policy template.

**August 5, 2011, June 20, 2008 and August 28, 2003:** Updates

**May 23, 2008:** The plan was first issued
VII. Exhibit A

Requirements for handling of customer Information relevant to interpretation of the GLB Safeguarding Rule, 16 CFR 314.2 see:

- Federal Trade Commission (FTC) Standards for Safeguarding Customer Information
- Cornell Law School Code of Federal Regulations (CFR) Title 16 Chapter 1 Subchapter C Part 314 Section 314.2

The definitions for following terms used in this plan:

- Collect
- Consumer
- Customer
- Customer relationship
- Financial product or service
- Nonpublic personal information
- Personally identifiable financial information

Are found from this link: Cornell Law School Code of Federal Regulations (CFR) Title 16 Chapter 1 Subchapter C Part 313 Section 313.3