Guideline on:	Safeguarding customer information related to financial products or services, including loans, financial advice or insurance.
Related Policy:	Not applicable
Effective Date:	June 20, 2008

Contact:	Robert Smith
Email:	Robert.Smith@ucop.edu
Phone #:	(510) 587-6244

I. SUMMARY

This guide is designed to promote University compliance with the Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act, or GLBA) and specifically with the GLBA Safeguarding Rule issued by the Federal Trade Commission. This applies to safeguarding customer information for loans to students, parents/guardians, and Workforce Members. It may apply to other financial transactions involving customer information (see III.E below).

UC entities and processes (whether or not they handle customer information as defined by the Federal Trade Commission (FTC) in Federal Register 16 CFR Part 313.3) are bound by current UC policies that govern information practices and security, including the Business & Finance Bulletins (BFB) for records management, privacy, Institutional Information and IT Resources. The FTC published an updated rule on December 9, 2021, with an effective date of January 10, 2022, with the exception of Section 314.4(a), (b)(1), (c)(1) through (8), (d)(2), (e), (f)(3), (h), and (i), effective December 9, 2022. This plan addresses the new rule.

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[1]: The GLBA Compliance Plan uses the term "customer information" as defined in the GLBA Safeguarding Rule, 16 CFR 314.2 (incorporating other definitions from the GLBA 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 (when stored with any of the following items below)

[1] UC's IS-3 Electronic Information Security Policy uses the term "Institutional Information" as an all-encompassing term. Institutional Information is classified by four Protection Levels. P1 is the lowest and P4 is the highest. Institutional Information related to GLBA is classified at either P3 or P4. IS-3 provides a set of security controls that manage cyber risk for this kind of data.

- Home address
- Home phone number
- Name of spouse or other relatives
- Citizenship
- Bank and credit card number(s)
- Income and credit histories
- Social Security numbers
- Performance evaluations or letter related to performance
- Any record containing nonpublic personal information about a customer handled or maintained by or on behalf of UC
- Other information within the GLBA definition of the "Nonpublic personal information"

III. GUIDANCE TEXT

A. UC GLBA 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 Workforce Members to protect sensitive information.

The University's written procedures for complying with the GLBA 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 Bulletin, IS-3 Electronic Information Security. Recognizing that UC customer information is now regularly, if not solely, found in electronic form, University compliance with GLBA is principally guided by IS-3 and its related standards.
- **GLBA Compliance Plan**. This Plan provides specific direction for Units that fall under the purview of the GLBA Safeguarding Rule.
    - It identifies the types of information subject to the GLBA Safeguarding Rule.
    - It directs that all electronic information must be handled in accordance with the University's comprehensive policy for protection of electronic information, Business and Finance Bulletin, IS-3 "Electronic Information Security (IS-3).
    - It clarifies expectations for the handling of paper records that are subject to the Rule and not covered in IS-3.
- **Systemwide Websites**. Information and resources pertinent to safeguarding information are available at the systemwide information security website.

- **Location Websites**. Location-specific procedures and guidance are provided on campus and UCOP websites devoted to information security. These may be found listed on the systemwide information security website.

B. Overview of Compliance Plan Requirements

Protection of Electronic Customer Information. IS-3 is the comprehensive systemwide policy for protecting electronic information[2]. Any UC Unit that handles GLBA customer information in electronic format, as defined in this document, must follow IS-3 to protect that data in accordance with the GLBA Safeguarding Rule. IS-3 and the related standards fully address the GLBA requirements for administrative, technical, and physical safeguards; risk assessment; Workforce Member training; and selection of and contracting with service providers with respect to electronic information. To avoid redundancy and confusion about precedence, this GLBA Compliance Plan purposefully does not duplicate IS-3 provisions, but rather expands upon them when necessary to ensure the University's full compliance with the GLBA Safeguarding Rule. GLBA customer information is classified at P3 or P4[3].

Protection of Customer Information in Paper Records. The Electronic Information Security policy, IS-3, does not address paper records. Therefore, specific guidance for ensuring that the University protects paper records containing customer information covered under the GLBA is provided in this plan. In summary, Units that handle GLBA customer information must ensure that their information security management program/plans, developed in accordance with IS-3, also address the handling of paper records, especially with respect to:

- Risk assessment and subsequent implementation of safeguards.
- Workforce Member training and management.
- Selection of and contracts with service providers, as well as testing, monitoring, and evaluation of safeguards.
- For both electronic and paper records—overall evaluation of the information security program and its effectiveness in protecting GLBA customer information.
- For both electronic and paper records—compliance with UC records retention policies.

C. UC GLBA Compliance Plan Coordinator (UCCPC)

The Vice President for Information Technology Services (VP-ITS) based at the UC Office of the President (UCOP) serves as the GLBA Compliance Plan Coordinator (UCCPC) for the UC system. In this capacity, the VP-ITS coordinates implementation of the program with Location-appointed officials, that by policy, have authority for financial management, information security, and records management. These include the Unit Heads, Unit Information Security Leads, and the Controller or a Controller-appointed GLBA Coordinator.

[2] Regarding electronic information, IS-3 uses the term "Institutional Information" and the related term "IT Resources."
[3] See the classification resources for more information. The GLBA use the term "Nonpublic Personal Information" (NPI). Transactional systems that create, store or process Customer Information must be classified at P4.

The UCCPC, along with the Location Chief Information Security Officer (CISO[4]), ensures that applicable Units 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 GLBA Compliance Plan.

In collaboration with the Locations CISOs, the UCCPC will create a written report to the Regents of the University of California on key aspects of the information security program and compliance with this plan at least once per year. The report must include the following information:

- The overall status of the information security program and UC's compliance with this plan.
- Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the information security program.

D. Qualified Individual (QI)

At each Location, the Cyber-risk Responsible Executive (CRE) must designate a "Qualified Individual" (QI) to oversee, implement, and enforce the Location's information security program. The QI is the Location CISO unless otherwise designated by the CRE.

The CRE is responsible for the direction and oversight of the QI.

The QI must complete a compliance review and provide a report to the systemwide CISO at least once per year. For the purposes for reporting to the Regents of the University of California, the Systemwide CISO is the qualified individual.

E. Scope of Applicability of the UC GLBA Compliance Plan

The UC GLBA Compliance Plan must be implemented by all organizations or Locations governed by the Regents of the University of California. It must also 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 GLBA Safeguarding Rule.

The types of financial services or products that are subject to the GLBA Safeguarding Rule are identified in Table 1. Units that handle the financial services or products, or the customer information pertaining to them during their operations, must comply with this plan and ensure appropriate safeguarding of the customer information using IS-3.

[4] Some Locations may name this role Information Security Officer (ISO).

Table 1: Applicability of the GLBA Safeguarding Rule at UC	
Financial Services or Products Covered by the GLBA Safeguarding Rule	**Examples of Units that May Handle These Services or Products**
►Student loans (bank loans, federal loans, UC loans) ►Emergency student loans (undergraduate and graduate) ►Parent/Guardian loans ►Repayable scholarships	►Financial Aid ►Student Accounts Receivable ►Student Loan Administration ►Billing ►Business Services ►Bursar's Office
►403(b) loans	►Human Resources ►Benefits
►Emergency faculty loans ►Emergency staff loans	►Billing ►Business Services ►Loans and Receivables
►Faculty and staff home loans	►Office of Loan Programs ►Payroll

In general, the Safeguarding Rule covers activities in which banks, by regulation, are authorized to engage. At UC, this translates principally to loans to students, parents/guardians, and Workforce Members.

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 GLBA 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; and 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, and payment plans for medical services.

Types of insurance that banks are not authorized to issue: student and Workforce Member health insurance and 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; and issuance of checks or electronic funds transfer (EFT) payments to students.

Credit Card or Debit Card Transactions: records obtained in connection with single or isolated financial transactions, such as ATM transactions or credit card

purchases.

F. Risk Assessment and Implementation of Safeguards

Units that handle data subject to the GLBA Safeguarding Rule must conduct periodic risk assessments and ensure that the assessments cover both paper records and electronic records. Guidance for 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, assess the sufficiency of safeguards in place to control these risks, and design and implement new or revised safeguards to control identified risks.

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

Design and Implementation of Safeguards. One of the outputs of the risk assessment is making recommendations to improve business controls and/or to implement additional information safeguards.

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

IS-3 Reference: III. 6. Risk Assessment, 8. Asset Inventory and Classification, and the Incident Response Standard.

G. Workforce Member Training and Management

Based on the results of risk assessments, Units must develop appropriate training programs to ensure staff is aware of protocols for protecting customer information. Training programs or materials must incorporate concepts relevant to both electronic and paper-based customer information, and build on information security concepts and requirements in IS-3.

Workforce Managers must keep Workforce Members informed about policies and programs that pertain to their work, including those that govern information security and privacy. Workforce Managers must ascertain which positions deal with customer information and assess whether these should be deemed “critical positions” that require background checks, as provided for by UC personnel policy.

Workforce Managers must ensure Workforce Members complete UC’s mandatory security awareness training as assigned.

IS-3 Reference. III.7 Human Resources Security.

H. Selection of Suppliers

Current University policies that govern agreements with third-party Suppliers:

(a) Require that these Suppliers adhere to applicable state and federal laws.

(b) Define requirements for the handling of data, including both the safeguarding of customer information, as required by the GLBA 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 Suppliers. Units seeking to contract with third parties to handle customer information must exercise due diligence to ensure that the Supplier is capable of maintaining appropriate safeguards for the information, in keeping with Business and Finance Bulletin IS-3, Electronic Information Security.

Contract Language. All agreements dealing with electronic records containing the customer information protected by the GLBA Safeguarding Rule must contain language to require, as necessary, the "safeguarding" of the University's customer information and notification in instances of incidents and/or breaches. Units engaging Suppliers must use the approved version of UC's Purchasing Agreement, Terms and Conditions, other applicable appendices, and Appendix Data Security.

Unit Heads initiating agreements with a Supplier who is handing paper records containing the customer information protected by the GLBA, must include a suitable statement-of-work clearly detailing the Supplier's obligations for the "safeguarding" of the University's customer information and notification in instances of incidents and/or breaches.

IS-3 Reference: III.15, Supplier Relationships.

Resources on Agreements and Contracts: Procurement Services

I. Program Evaluation

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

Under this Plan, Units are responsible for the routine testing, monitoring, and evaluation of safeguards implemented by the Unit to minimize identified risks. This is accomplished primarily through routine self-assessments by Units and the University's scheduled internal audits.

Location 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. The Internal Audit Program periodically audits business functional areas such as cash management, accounts payable, financial aid, fundraising and gift processing, student fees and receivables, disbursements, and medical billing and receivables. These functional areas overlap with areas identified for compliance

with the GLBA Compliance Plan. Internal audits incorporate an evaluation of implementation of the GLBA Compliance Plan and the implementation of IS-3 to review compliance with policy, adequacy of risk management, management information flow, and business effectiveness and efficiency.

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

IS-3 References: Section III:

- 5. Information Security Management Program
- 6. Risk Management Process
- 7. Human Resource Security
- 8. Asset Management
- 9. Access Control
- 10. Encryption
- 11. Physical and Environmental Security
- 12. Operations Management
- 13. Communications Security
- 14. System Acquisition, Development and Maintenance
- 15. Supplier Relationships
- 16. Information Security Incident Management
- 17. Information Security Aspects of Business Continuity
- 18. Compliance and External Requirements

IS-3 Standard References:

- Incident Response Standard
- Other Standards

IV. COMPLIANCE/RESPONSIBILITIES

The Vice President for Information Technology Services serves as the systemwide GLBA Compliance Plan Coordinator. This role is responsible for systemwide compliance with the GLBA Safeguarding Rule through appropriate communication and coordination with the Locations’ Controllers, CISOs, and CIOs.

Unit Heads and Unit Information Security Leads (UISL) must comply with the GLBA

Safeguarding Rule and are responsible for establishing the processes by which their Workforce Members comply with Business and Finance Bulletin IS-3 Electronic Information Security. They are also responsible for incorporating specific requirements of this plan into the Unit's IS-3 information security program. Separately, Units are responsible for creating procedures for the protection of customer information found in paper records.

Workforce Managers and supervisors are responsible for ensuring that Workforce Members are:

(a) Aware of and understand how to implement their Unit's information security program and other applicable policies and programs.

(b) Appropriately trained in compliance, including detecting, handling, and reporting security breaches and incidents.

Location CISOs can assist Unit Heads with setting risk evaluation schedules and processes as requested.

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

Workforce Members and Workforce Managers are responsible for complying with IS-3.

All University Workforce Members are responsible for conducting their work in accordance with University policies and procedures, and 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 Workforce Members 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. This includes, but is not limited to, a student's name, the name of a student's parent/guardian 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 Workforce Members 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-3 Electronic Information Security

- UC's Electronic Information Security Policy (IS-3) allows it to protect confidentiality; to maintain the integrity of all data created, received, or collected by UC (Institutional Information); to meet legal and regulatory requirements; and to ensure timely, efficient, and secure access to Institutional Information and IT Resources).
- IS-3 applies to all UC campuses and medical centers, the UC Office of the President, UC Agriculture and Natural Resources, UC-managed national laboratories, and all other UC Locations. The policy also applies to all Workforce Members, Suppliers, Service Providers, and other authorized users.
- IS-3 establishes a framework that ensures all UC Locations follow the same approach to reduce and manage cyber risk, protect information, and support the proper functioning of IT Resources. This consistent approach also positions UC Locations to collaborate on cybersecurity. The policy also supports local flexibility and control while promoting systemwide consistency and collaboration. Key features supporting local control include an exception process and a Risk Treatment Plan, a tool that creates a flexible and scalable approach to cybersecurity.
- Protection Level and Availability Level classifications guide the implementation of the policy. These levels range from P1, the lowest, to P4, the highest. When the classification is high, more effort goes into protecting the asset. These classifications also inform IS-3's risk-based approach to security.
- Customer Information (a type of Institutional Information) is classified as Protection Level 4 (P4) in the UC Classification Guide. P4 Institutional Information must be protected using the framework of controls identified in IS-3 III. 7-18 and adjusted based on the risk management process, III. 6.
- Unit Heads selecting and using Suppliers handling Customer Information must endure III.15 Supplier Relationships is followed.

B&F Bulletin IS-12 IT Recovery

- Locations are required by the UC Policy on Safeguards, Security, and Emergency Management to have a comprehensive emergency management program. One of the key aspects of emergency management is a continuity of operations plan. UC has commonly adopted the title "Business Continuity Plan" (BCP) as the working name for this document.
- This policy follows that convention. BCP is the process for developing procedures to sustain business operations while recovering from a significant disruption. IT Recovery must align with Location BCP objectives. The Location uses its BCP and Business Impact Analysis (BIA) to determine what business processes (Units) are in-scope for IT Recovery planning. The BCP and BIA

result from the execution of the Policy on Safeguards, Security, and Emergency Management. UC recognizes that a certain level of risk may be accepted through the Location governance processes.

- This policy specifies the duties of Workforce Members responsible for the IT Recovery process. Successful execution of an IT Recovery strategy requires commitment and planning involving Location senior management and Unit Heads.
- The CRE oversees funding, risk tolerance, and planning for the Location. The Unit Head oversees funding and planning for the Unit.
- Additionally, UC has adopted five Recovery Levels (R1 to R5) ranging from 30 days (R1) to 15 minutes (R5).

B&F Bulletin RMP-7 Privacy of and Access to Information Responsibilities

- 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

- Exhibit A, “Securing the Services of Independent Consultants,” 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 must 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 must 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 must be considered Confidential Information.”

B&F Bulletin BUS 43 Purchases of Goods and Services; Supply Chain Management

- Related to Purchase Transactions – Executing Officials:
    - Must 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.

- Must reject bids that are non-responsive or that are from a bidder who is not responsible.

- References the UC Terms and Conditions of Purchase which requires:
  - Supplier to agree 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 must control the UC Terms and Conditions of Purchase and any document to which it is appended.

VI. REVISION HISTORY

March 16, 2022: Updated to reflect the FTC's revised safeguards rule published in the Federal Register, Vol. 86, No. 234, Thursday, December 9, 2021.

November 4, 2021: Updated to reflect policy revisions and retirements. Since 2017, IS-3 and IS-12 have been rewritten. IS-3 is now accompanied by nine standards. IS-2 was retired. Terms were updated to be consistent with policy conventions. Some responsibilities were updated to align with the policy work noted above. Hyperlinks were also updated. Fixed accessibility issues, formatting, and other small errors. This version was circulated and reviewed, but not posted because the FTC issued a new rule on December 9, 2021.

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

May 23, 2003: The plan was first issued.

VII. Exhibit A

For requirements for handling of Customer Information relevant to interpretation of the GLBA Safeguarding Rule, 16 CFR 314.2, see the following:

- https://www.federalregister.gov/documents/2021/12/09/2021-25736/standards-for-safeguarding-customer-information
- 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
- Guidance: Authentication and Access to Financial Institution Services and Systems (Use IS-3 for implementation of this guidance)

The definitions used in this plan for the following terms:

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

are found at this link: Cornell Law School Code of Federal Regulations (CFR) Title 16 Chapter1 Subchapter C Part 313 Section 313.3

The definitions used in this plan for the following terms from § 314.2:

- Authorized user
- Customer information
- Customer relationship
- Encryption
- Information system[5]
- Multi-factor authentication
- Nonpublic personal information
- Penetration testing
- Security event
- Service provider[6]

[5] IS-3 see IT Resource.
[6] IS-3 see Supplier.

are found at this link: https://www.law.cornell.edu/cfr/text/16/314.2

Summary of new requirements outlined in the December 9, 2021 Rule

These control objectives are covered in the IS-3 Electronic Information Security policy and this plan. These must be implemented by December 9, 2022.

314.4(a)—Designate a "qualified individual[7]" to oversee, implement, and enforce the institution's information security program.

314.4(b)(1)—Produce a written risk assessment about the institution's customer information that includes a now-mandated set of criteria and requirements.

314.4(c)(1)-(8)—"Design and implement safeguards to control the risks you identity through risk assessment," including the following:

- Technical and physical access controls to ensure only authorized access.
- An inventory of all relevant parts of the IT environment and management of the same consistent with their business priority and the institution's risk strategy.
- Encryption of all customer information in transit over external networks and at rest.
- Procedures for securely developing internal applications and assessing the security of externally developed applications used in relation to customer information.
- Multi-factor authentication for any individual accessing any information system.
- Procedures for the secure disposal of customer information that is no longer needed for business operations or another legitimate business purpose.
- Change management procedures.
- Measures to monitor and log the activities of authorized users and to detect their unauthorized access or use of or tampering with customer information.

314.4(d)(2)—Implement continuous monitoring of "information systems" (as defined in 314.2) or annual penetration testing with vulnerability assessments at least every six months.

314.4(e)—Establish policies and procedures to ensure that your staff receives security awareness training, that you hire qualified information security personnel and provide ongoing professional development for them, and that key members of your information security staff maintain their knowledge of current threats and responses.

314.4(f)(3)—Periodically assess the information security risks that your institution's service providers present and the adequacy of the safeguards they deploy to ensure that they are following the provisions of the Rule.

[7] At the Location, this is the Location CISO.

314.4(h)—Establish a written incident response plan, including a set of specific elements, for the customer information that the institution controls.

314.4(i)—Require your institution's "qualified individual[8]" to submit a written report on key aspects of the information security program to the institution's governing board at least once per year.

[8] For the purposes of systemwide reporting to the Regents of the University of California, this is the Systemwide CISO.