

GRAMM LEACH BLILEY INFORMATION SECURITY PROGRAM

CALIFORNIA STATE UNIVERSITY, LOS ANGELES

Federal regulations are mandating new privacy protections to help safeguard “customer information” in the possession of financial institutions. A portion of these regulations are applicable to colleges and universities and requires that we establish and periodically revise an information security program.

The following document sets forth a GLB Information Security Plan for California State University, Los Angeles. It should serve as a guide for how information security is to be maintained at this campus. If you have any questions or concerns about this plan, please contact University Counsel/Information Practices Officer Victor I. King at extension 323-343-3054.

I. Definitions

Covered Data and Information for the purpose of this document include, but are not limited to, personally identifiable information (e.g., first and last name, social security number, date of birth, home address, home telephone number, academic performance record, physical description, medical history, disciplinary history, gender, and ethnicity) and personal financial information (e.g., Student Financial Information, credit card numbers, bank account numbers, including PIN numbers and access codes). Covered Data and Information includes both paper and electronic records, including that contained on any external media devices such as flash drives, CDs, and backup devices.

Financial Information is that information that the University has obtained from employees, alumni, auxiliary agencies, patrons, external program participants, or the like in the process of offering a financial product or service, or conducting a program. Offering a financial product or service, or conducting a program includes, but is not limited to, compiling billing information for patrons of venues and events, billing for services to employees or community participants, employee and alumni donations, tracking of financial and other confidential information on internal and external programs. Examples of Financial Information include bank and credit card account numbers and income and credit histories.

Student Financial Information is that information the University has obtained from a student in the process of offering a financial product or service, or such information provided to the University by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 CFR § 225.28. Examples of Student Financial Information include bank and credit card account numbers and income and credit histories.

GRAMM LEACH BLILEY INFORMATION SECURITY PROGRAM

CALIFORNIA STATE UNIVERSITY, LOS ANGELES

II. Relevant Areas

The following offices have been identified as relevant areas to be considered when assessing the risks to customer information:

- Accounts Receivable Office
- Administrative Technology
- Admissions
- Alumni Relations
- Athletics
- Business Financial Services
- Career Development Center
- Cashiers (Registers and terminals)
- Charter College of Education, office handling student credentials
- Clinics (Audiology, Speech, and Kinesiology)
- Commuter Services
- Extended Education
- Financial Aid Office
- Golden Eagle Card Office
- Housing Services
- Human Resources Management
- Information Technology Services
- Institutional Research
- Institutional Review Board
- Library
- Office for Students with Disabilities
- Office of Graduate Studies and Research
- Offices of the College Deans
- Payroll Office
- Registrar's Office
- Risk Management and Environmental, Health and Safety Office
- Student Affairs – all programs (i.e., GEAR-UP, Upward Bound, International Students, EOP)
- Student Health Center
- Student Financial Services
- Testing Office
- University Development
- University Police

In addition to the above areas, all offices and individuals campus-wide who are engaged in the following activities or practices are required to assess their risk of customer information.

GRAMM LEACH BLILEY INFORMATION SECURITY PROGRAM

CALIFORNIA STATE UNIVERSITY, LOS ANGELES

Academic and administrative offices that handle electronic or printed personnel records, financial records, transactional records, or student records
Academic and administrative offices that transmit confidential information to off-site locations as part of a periodic review or submission requirement
Centers and Institutes that provide services and acquire personal or financial information from participants or constituents
Faculty serving as directors, coordinators, principal investigators, or program directors for programs collecting confidential information
Faculty, staff, and administrators with contracts to use, access, or provide confidential information to or receive from a non-campus entity (e.g., government databases, science databases)
Performing arts organizations that collect patron information.

III. Gramm Leach Bliley (GLB) Requirements

GLB mandates that the University appoint an information security coordinator, conduct a risk assessment of likely security and privacy risks, 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 Program periodically.

IV. Information Security Officers

The campus has designated two Information Security Officers – University Counsel and the Director of IT Security and Compliance. The Information Security Officers will coordinate with the Internal Auditor's Office to maintain the GLB information security program. The University Counsel/Information Practices Officer will provide guidance in complying with all privacy regulations.

V. Relevant Areas' Supporting Information Security Program

Each Relevant Area outlined above is responsible for securing customer information in accordance with all privacy guidelines. A written security policy that details the information security policies and processes will be maintained by each Relevant Area and will be made available to the University Counsel/Information Practices Officer or Internal Auditor's office upon request. In addition, the Information Technology Services division will maintain and provide access to policies and procedures that protect against any anticipated threats to the security or integrity of electronic customer information and that guard against the unauthorized use of such information.

GRAMM LEACH BLILEY INFORMATION SECURITY PROGRAM

CALIFORNIA STATE UNIVERSITY, LOS ANGELES

VI. Risk Assessment and Safeguards

- A. The Information Security Officers must work with all Relevant Areas to identify potential and actual risks to security and privacy of Covered Data and Information. The head of each Relevant Area, or designee, will conduct an annual data security review, with guidance from the Information Security Officers. Vice Presidents will be asked to identify any employees in their respective areas that work with Covered Data and Information. In addition, Information Technology Services (ITS) will conduct a quarterly review of procedures, incidents, and responses. ITS will assure that procedures and responses are appropriately reflective of those widely practiced at other universities.
- B. ITS shall strive to assure that patches for the software environments (e.g., operating system, system software, database management systems, and application packages) for centrally managed servers (e.g., human resources, financial, student administration, electronic mail, Web services, course management, and directory) and centrally managed desktops and laptops are reasonably up-to-date, and will keep records of patching activity. ITS will review its procedures for patches to its software environments at least annually and will keep current on potential threats to the network and its data. Risk assessments will be updated quarterly. The Information Security Officers will work with other areas of the University to develop guidelines for the maintenance and management of the software environments of any servers connected to the campus network but located outside the central server area.
- C. ITS shall strive to assure the physical security of all centrally managed servers which contain or have access to Covered Data and Information. The Information Security Officers will develop appropriate physical security guidelines and work with other areas of the University to ensure they meet the physical security guidelines for any servers connected to the campus network but located outside the central server area. ITS has primary responsibility for the assessment of internal and external risks to information security, but all members of the University community must be involved in risk assessment. ITS, working in conjunction with each Relevant Area, will conduct regular risk assessments, including but not limited to the categories listed by GLB.
- D. Relevant Areas will develop a listing of persons responsible for each covered data field in systems, databases, documents, file cabinets, electronic storage media, laptops and computers contained in their area. This listing must be submitted to the Information Security Officers initially upon completion of the first review, and immediately as changes occur thereafter. ITS and the Relevant Areas will conduct ongoing audits, and will report any significant questionable activities, which may compromise security of Covered Data and Information.

GRAMM LEACH BLILEY INFORMATION SECURITY PROGRAM

CALIFORNIA STATE UNIVERSITY, LOS ANGELES

- E. ITS will work with the Relevant Areas to develop and maintain a registry of those members of the University community who have access to Covered Data and Information contained in the Student Administration and Contributor Relations systems. Administration and Finance will work with the Relevant Areas to develop and maintain a registry of those members of the University community who have access to Covered Data and Information contained in the Human Resources Management and Financials systems. ITS and Administration and Finance will work to keep this registry up to date. Human Resources Management is responsible for including the original user's account request form in each employee's official personnel file.
- F. ITS, with assistance from Public Safety, will assure the physical security of all centrally managed servers and terminals, which contain or have access to Covered Data and Information. ITS will work with other areas of the University to develop guidelines for physical security of any covered servers in locations outside the central server area. All areas with servers outside the central server area must sign and submit an ITS Memo of Understanding outlining server security requirements prior to the approval of new server procurements. The Vice Presidents will conduct a survey of other physical security risks, including the storage of covered paper records in non-secure environments, and other procedures, which may expose the University to risks.
- G. Social security numbers are considered protected information under both GLB and the Family Educational Rights and Privacy Act (FERPA). By necessity, student social security numbers are in the University student information system. The Vice Presidents will conduct an assessment of access and use of social security numbers by the University, subcontractors with such access, and auxiliaries.
- H. ITS will develop a written guideline to ensure that all electronic Covered Data and Information is encrypted in transit and that the central databases are protected from security risks. Relevant Areas are responsible for contacting IT Security Management and Compliance for assistance prior to transmitting approved Covered Data and Information to off-site locations.
- I. ITS will develop written plans and procedures to detect and respond to actual or attempted attacks on Covered Data and Information systems.
- J. The Vice President for Institutional Advancement will periodically review the University's disaster recovery program and data-retention policies and present a report to the President or his designee.

GRAMM LEACH BLILEY INFORMATION SECURITY PROGRAM

CALIFORNIA STATE UNIVERSITY, LOS ANGELES

VII. Employee Training and Education

While the heads of Relevant Areas are ultimately responsible for ensuring compliance with information security practices, ITS and Human Resources Management will each work to develop training and education programs for all employees who have access to Covered Data and Information. These employees typically fall into three categories: professionals in information technology who have general access to all University data; custodians of data as identified in the data handbook; and those employees who use the data as part of their essential job duties.

VIII. Oversight of Service Providers and Contracts.

California State University, Los Angeles, will select appropriate service providers that are given access to customer information in the normal course of business and will contract with them to provide adequate safeguards. In the process of choosing a service provider that will have access to customer information, the evaluation process shall include the ability of the service provider to safeguard customer information. Contracts with service providers will include, to the extent possible, the following provisions: an explicit acknowledgment that the contract allows the contract partner access to confidential information; 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 provision requiring immediate notification in the event a campus-assigned employee terminates employment; 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 California State University, Los Angeles, to immediately terminate the contract without penalty; 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 agreement.

The Director of Procurement and Contracts, the Vice President for Administration and Finance and CFO, and/or University Counsel/Information Practices Officer are responsible for reviewing service provider contracts for the University and for ensuring all provisions are incorporated into contracts prior to award.

GRAMM LEACH BLILEY INFORMATION SECURITY PROGRAM

CALIFORNIA STATE UNIVERSITY, LOS ANGELES

Service providers requiring a system account and/or password to perform maintenance on University computer systems must complete a California State University, Los Angeles Third Party Access Form and sign a confidentiality agreement. Such service providers will be required to provide notice of any terminations of personnel dedicated to providing full-time campus or backup support.

IX. Security Breach Notification

The Information Security Officers will work closely with the Vice President of Information Technology Services and CTO and the University Counsel/Information Practices Officer to ensure that the campus complies with applicable law regarding notification of security breaches involving confidential information.

X. Evaluation and Revision of the Information Security Program

This GLB information security plan shall be evaluated and adjusted in light of relevant circumstances, including changes in the University's business arrangements or operations, or as a result of testing and monitoring the safeguards. Periodic auditing of each Relevant Area's compliance shall be done per the internal auditing schedule. Annual risk assessment will be done through the Internal Auditor's Office. Evaluation of the risk of new or changed business arrangements will be done through the University Counsel/Information Practices Officer.

GRAMM LEACH BLILEY INFORMATION SECURITY PROGRAM

Appendix A

Roles and Responsibilities (<i>Section Reference</i>)	Timeframe
<p><u>University Counsel/ Information Practices Officer</u></p> <ol style="list-style-type: none"> 1. Handle questions and concerns related to the Gramm Leach Bliley (GLB) Information Security Program. (<i>Introduction</i>) 2. Provide guidance to the campus in complying with all privacy regulations. (<i>IV</i>) 3. Review all service provider contracts that give access to customer information in the normal course of business and ensure all provisions of section VII are incorporated into contracts prior to award. (<i>VIII</i>) 4. Evaluate the risk of new or changed business arrangements. (<i>X</i>) 	<ol style="list-style-type: none"> 1. Ongoing 2. Ongoing 3. Ongoing 4. Annually
<p><u>Information Security Officers</u></p> <ol style="list-style-type: none"> 1. Coordinate with the Internal Auditor's Office to maintain the GLB Information Security Program. (<i>IV</i>) 2. Work with all "Relevant Areas" to identify potential and actual risks. (<i>VI.A</i>) 3. Work with other areas of the University to develop guidelines for maintenance and management of servers connected to the network, but located outside the central server area. (<i>VI.B</i>) 4. Develop physical security guidelines and work with other areas with servers located outside the central server area to ensure they meet the physical security guidelines. (<i>VI.C</i>) 5. Work with the Vice President for ITS and CTO and the University Counsel/Information Practices Officer to ensure the campus complies with applicable laws regarding notification of security breaches. (<i>IX</i>) 	<ol style="list-style-type: none"> 1. Ongoing 2. Immediate 3. Ongoing 4. Immediate and ongoing 5. Ongoing
<p><u>Internal Auditor's Office</u></p> <ol style="list-style-type: none"> 1. Conduct a campus-wide risk assessment and compliance review of each "Relevant Area." (<i>X</i>) 	<ol style="list-style-type: none"> 1. Annually
<p><u>President's Office</u></p> <ol style="list-style-type: none"> 1. Identify all "Relevant Areas" as defined in section II that operate within the division. (<i>VI</i>) 2. Identify the leader of each "Relevant Area" or the responsible designee. (<i>VI</i>) 3. Identify any employees that work with "Covered Data and Information" in the division. (<i>VI.A</i>) 4. Instruct each "Relevant Area" to develop a listing of persons responsible for each covered data field in systems, databases, documents, file cabinets, electronic storage media, laptops and computers contained in the area. (<i>VI.D</i>) 5. Assess internal and external risks to information security within the division. (<i>VI.C</i>) 	<ol style="list-style-type: none"> 1. Immediate 2. Immediate 3. Immediate 4. Immediate 5. Ongoing
<p><u>Provost and Vice President for Academic Affairs</u></p> <ol style="list-style-type: none"> 1. Identify all "Relevant Areas" as defined in section II that operate within the division. (<i>VI</i>) 2. Identify the leader of each "Relevant Area" or the responsible designee. (<i>VI</i>) 3. Identify any employees that work with "Covered Data and Information" in the division. (<i>VI.A</i>) 4. Instruct each "Relevant Area" to develop a listing of persons responsible for each covered data field in systems, databases, documents, file cabinets, electronic storage media, laptops and computers contained in the area. (<i>VI.D</i>) 5. Assess internal and external risks to information security within the division. (<i>VI.C</i>) 6. Instruct all areas with servers located outside the central server area that they must sign and submit an ITS Memo of Understanding (MOU) outlining server security requirements prior to the approval of new server procurements. (<i>VI.F</i>) 7. Conduct a survey of other physical security risks, including storage of covered paper records in non-secure environments, and other procedures, which may expose the campus to risks. (<i>VI.F</i>) 8. Conduct an assessment of access and use of social security numbers by the University, subcontractors with such access, and auxiliaries. (<i>VI.G</i>) 	<ol style="list-style-type: none"> 1. Immediate 2. Immediate 3. Immediate 4. Immediate 5. Ongoing 6. Immediate 7. Immediate 8. Immediate

GRAMM LEACH BLILEY INFORMATION SECURITY PROGRAM

Appendix A

<p><u>Vice President for Administration and Finance and CFO</u></p> <ol style="list-style-type: none"> 1. Identify all “Relevant Areas” as defined in section II that operate within the division. <i>(VI)</i> 2. Identify the leader of each “Relevant Area” or the responsible designee. <i>(VI)</i> 3. Identify any employees that work with “Covered Data and Information” in the division. <i>(VI.A)</i> 4. Instruct each “Relevant Area” to develop a listing of persons responsible for each covered data field in systems, databases, documents, file cabinets, electronic storage media, laptops and computers contained in the area. <i>(VI.D)</i> 5. Assess internal and external risks to information security within the division. <i>(VI.C)</i> 6. In conjunction with “Relevant Areas,” develop and maintain a registry of employees who have access to “Covered Data and Information” in Financials and Human Resource Management systems. <i>(VI.E)</i> 7. Instruct all areas with servers located outside the central server area that they must sign and submit an ITS Memo of Understanding (MOU) outlining server security requirements prior to the approval of new server procurements. <i>(VI.F)</i> 8. Conduct a survey of other physical security risks, including storage of covered paper records in non-secure environments, and other procedures, which may expose the campus to risks. <i>(VI.F)</i> 9. Conduct an assessment of access and use of social security numbers by the University, subcontractors with such access, and auxiliaries. <i>(VI.G)</i> 10. Review all service provider contracts that give access to customer information in the normal course of business and ensure all provisions of section VII are incorporated into contracts prior to award. <i>(VIII)</i> 	<ol style="list-style-type: none"> 1. Immediate 2. Immediate 3. Immediate 4. Immediate 5. Ongoing 6. Immediate 7. Immediate 8. Immediate 9. Immediate 10. Ongoing
<p><u>Vice President for Information Technology Services and CTO</u></p> <ol style="list-style-type: none"> 1. Identify all “Relevant Areas” as defined in section II that operate within the division. <i>(VI)</i> 2. Identify the leader of each “Relevant Area” or the responsible designee. <i>(VI)</i> 3. Identify any employees that work with “Covered Data and Information” in the division. <i>(VI.A)</i> 4. Instruct each “Relevant Area” to develop a listing of persons responsible for each covered data field in systems, databases, documents, file cabinets, electronic storage media, laptops and computers contained in the area. <i>(VI.D)</i> 5. Maintain and provide access to policies and procedures that protect against any anticipated threats. <i>(V)</i> 6. Conduct a review of procedures, incidents, and responses. <i>(VI.A)</i> 7. Ensure that a patch management program is in place for centrally managed servers, e-mail servers, Web servers, course management servers, directory servers, and centrally managed desktops and laptops. Keep records of all patching activities. <i>(VI.B)</i> 8. Review the patch management program procedures to ensure they remain current with changing threats. <i>(VI.B)</i> 9. Assure the physical security of centrally managed servers that contain “Covered Data and Information.” <i>(VI.C)</i> 10. Assume primary responsibility for assessment of internal and external risks to information security for the campus. <i>(VI.C)</i> 11. Conduct regular risk assessments. <i>(VI.C)</i> 12. In conjunction with “Relevant Areas,” develop and maintain a registry of employees who have access to “Covered Data and Information” in Student Administration and Contributor Relations systems. <i>(VI.E)</i> 13. In conjunction with Public Safety, assure the physical security of centrally managed servers and terminals that contain “Covered Data and Information.” <i>(VI.F)</i> 14. Work with other campus areas to develop guidelines for physical security of covered servers outside the central server area. <i>(VI.F)</i> 15. Instruct all areas with servers located outside the central server area that they must sign and submit an ITS Memo of Understanding (MOU) outlining server security requirements prior to the approval of new server procurements. <i>(VI.F)</i> 16. Conduct a survey of other physical security risks, including storage of covered paper records in non-secure environments, and other procedures, which may expose the campus to risks. <i>(VI.F)</i> 	<ol style="list-style-type: none"> 1. Immediate 2. Immediate 3. Immediate 4. Immediate 5. Ongoing 6. Quarterly 7. Ongoing 8. Yearly 9. Ongoing 10. Ongoing 11. Yearly 12. Immediate and ongoing 13. Ongoing 14. Ongoing 15. Immediate 16. Immediate

GRAMM LEACH BLILEY INFORMATION SECURITY PROGRAM

Appendix A

<ul style="list-style-type: none"> 17. Conduct an assessment of access and use of social security numbers by the University, subcontractors with such access, and auxiliaries. <i>(VI.G)</i> 18. Develop written guidelines to ensure all electronic “Covered Data and Information” is encrypted in transit and that central databases are protected. <i>(VI.H)</i> 19. Develop written plans and procedures to detect and respond to actual or attempted attacks on “Covered Data and Information” systems. <i>(VI.I)</i> 20. In conjunction with Human Resources Management, develop a training and education program for all employees who have access to “Covered Data and Information.” <i>(VII)</i> 	<ul style="list-style-type: none"> 17. Immediate 18. Immediate 19. Immediate 20. Immediate
<p><u>Vice President for Institutional Advancement</u></p>	
<ul style="list-style-type: none"> 1. Identify all “Relevant Areas” as defined in section II that operate within the division. <i>(VI)</i> 2. Identify the leader of each “Relevant Area” or the responsible designee. <i>(VI)</i> 3. Identify any employees that work with “Covered Data and Information” in the division. <i>(VI.A)</i> 4. Instruct each “Relevant Area” to develop a listing of persons responsible for each covered data field in systems, databases, documents, file cabinets, electronic storage media, laptops and computers contained in the area. <i>(VI.D)</i> 5. Assess internal and external risks to information security within the division. <i>(VI.C)</i> 6. Instruct all areas with servers located outside the central server area that they must sign and submit an ITS Memo of Understanding (MOU) outlining server security requirements prior to the approval of new server procurements. <i>(VI.F)</i> 7. Conduct a survey of other physical security risks, including storage of covered paper records in non-secure environments, and other procedures, which may expose the campus to risks. <i>(VI.F)</i> 8. Conduct an assessment of access and use of social security numbers by the University, subcontractors with such access, and auxiliaries. <i>(VI.G)</i> 9. Review the University’s disaster recovery program and data retention policies and present a report to the President or his designee. <i>(VI.J)</i> 	<ul style="list-style-type: none"> 1. Immediate 2. Immediate 3. Immediate 4. Immediate 5. Ongoing 6. Immediate 7. Immediate 8. Immediate 9. Annually
<p><u>Vice President for Student Affairs</u></p>	
<ul style="list-style-type: none"> 1. Identify all “Relevant Areas” as defined in section II that operate within the division. <i>(VI)</i> 2. Identify the leader of each “Relevant Area” or the responsible designee. <i>(VI)</i> 3. Identify any employees that work with “Covered Data and Information” in the division. <i>(VI.A)</i> 4. Instruct each “Relevant Area” to develop a listing of persons responsible for each covered data field in systems, databases, documents, file cabinets, electronic storage media, laptops and computers contained in the area. <i>(VI.D)</i> 5. Assess internal and external risks to information security within the division. <i>(VI.C)</i> 6. Instruct all areas with servers located outside the central server area that they must sign and submit an ITS Memo of Understanding (MOU) outlining server security requirements prior to the approval of new server procurements. <i>(VI.F)</i> 7. Conduct a survey of other physical security risks, including storage of covered paper records in non-secure environments, and other procedures, which may expose the campus to risks. <i>(VI.F)</i> 8. Conduct an assessment of access and use of social security numbers by the University, subcontractors with such access, and auxiliaries. <i>(VI.G)</i> 	<ul style="list-style-type: none"> 1. Immediate 2. Immediate 3. Immediate 4. Immediate 5. Ongoing 6. Immediate 7. Immediate 8. Immediate
<p><u>Director of Human Resources Management</u></p>	
<ul style="list-style-type: none"> 1. Ensure that Human Resources Management includes the applicant’s original request form in each employee’s official personnel file. <i>(VI.E)</i> 2. In conjunction with Information Technology Services, develop a training and education program for all employees who have access to “Covered Data and Information.” <i>(VII)</i> 	<ul style="list-style-type: none"> 1. Ongoing 2. Immediate

GRAMM LEACH BLILEY INFORMATION SECURITY PROGRAM

Appendix A

<p><u>Director of Procurement and Contracts</u></p> <ol style="list-style-type: none"> 1. Ensure that all procurements for servers located outside the centrally managed server area (ITS data center) have an attached Memo of Understanding with appropriate approval signatures. (VI.F) 2. Review all service provider contracts that give access to customer information in the normal course of business and ensure all provisions of section VII are incorporated into contracts prior to award. (VIII) 	<ol style="list-style-type: none"> 1. Ongoing 2. Ongoing
<p><u>Director of Public Safety</u></p> <ol style="list-style-type: none"> 1. In conjunction with ITS, assure the physical security of centrally managed servers and terminals that contain “Covered Data and Information.” (VI.F) 	<ol style="list-style-type: none"> 1. Ongoing
<p><u>“Relevant Area” leader or designee</u></p> <ol style="list-style-type: none"> 1. Prepare a written Department GLB Information Security Program that details the information security policies and processes that will be maintained to secure customer information in accordance with all privacy guidelines. (V) 2. Submit the Department GLB Information Security Program to University Counsel/Information Practices Officer or Internal Audit as requested. (V) 3. Conduct an annual data security review. (VI.A) 4. Develop and maintain a listing of persons responsible for each covered data field in systems, databases, documents, file cabinets, electronic storage media, laptops and computers contained in the area. (VI.D) 5. Submit item 4 to the Information Security Officers upon completion of the first review and immediately thereafter as changes occur. (VI.D) 6. Conduct periodic audits and report any significant questionable activities. (VI.D) 7. Contact IT Security Management and Compliance for assistance prior to transmitting approved “Covered Data and Information” to off-site locations. (VI.H) 	<ol style="list-style-type: none"> 1. Immediate 2. As requested 3. Annually 4. Immediate 5. Immediate and ongoing 6. Ongoing 7. Ongoing
<p><u>Service Providers</u></p> <ol style="list-style-type: none"> 1. Complete a California State University, Los Angeles <i>Third Party Access Form</i> and sign a confidentiality agreement if a system account and/or password are required to perform system maintenance. (VIII) 2. Provide immediate notice of personnel terminations to the campus. (VIII) 	<ol style="list-style-type: none"> 1. Immediate and ongoing 2. Ongoing