



# CALIFORNIA STATE UNIVERSITY, LONG BEACH

Subject: <b>Third Party Agreements/Confidential Information</b>	
Department: <b>Information Security Management and Compliance</b>	Reference No.:
Division: <b>Administration and Finance</b>	Issue Date: <b>April 2007</b>
References: <b>• Gramm-Leach-Bliley Act; FTC-15USC Subchapter I, §6801-6809 &amp; Subchapter II, §6821-6827</b>	Revision Date: <b>October 2007</b>
Web Links: <b>• <a href="http://daf.csulb.edu/offices/vp/information_security">http://daf.csulb.edu/offices/vp/information_security</a></b>	Expiration Date: <b>N/A</b>

## I. BACKGROUND

Federal legislation designed to ensure the privacy and safeguarding of confidential information places specific requirements on the University when the University allows access to or shares custody of its confidential information with third parties. Third parties may include those who store or destroy confidential information; conduct forensic investigation of electronic data; or conduct other electronic communication services.

## II. STANDARD

California State University, Long Beach shall take reasonable measures to select and retain third parties that are capable of maintaining appropriate safeguards for the information at issue; and shall require each third party, by written Agreement, to implement and maintain such safeguards. The University shall not contractually engage a third party who cannot demonstrate that they are capable of maintaining appropriate safeguards to protect information or who cannot demonstrate that they maintain required insurance coverage.

When Agreements are established with contractors, consultants, or external vendors, (third parties) those Agreements shall include satisfactory assurances that the contracting third party will appropriately safeguard information in accordance with federal and state laws and regulations and University policies. When providing access to or passing confidential information to a third party agent of the University, the written contractual Agreements shall include terms and conditions that:

- prevent disclosure of confidential information by the third party to other third parties including subcontractors,
- require third parties to observe federal and state laws and University policies for privacy and security,
- require a specific plan by the third party for the implementation of administrative, technical, or physical security strategies to protect CSULB confidential information,
- require a plan for the destruction or return of confidential information upon completion of the third party's contractual obligations,
- specify access or authorization permissions and restrictions necessary to fulfill contractual obligations.

Access shall be terminated when contractual obligations have been completed.

## III. PROCEDURES

The following requirements govern Agreements with third-parties in those instances where the third party may have access to confidential information:

- A. Prior to the University entering into contractual agreement with a third party, the Purchasing Office shall determine the adequacy of the third party's system of safeguarding information. Depending on the service to be provided, the University may consider reviewing the third party's audits, summaries of its test results for security, or other internal and external security evaluations. The Purchasing Office may be aided in this determination by the University Risk Manager, Internal Auditing Services, and/or Information Technology Services.

- B.** After the third party's system of safeguarding information has been determined to be adequate, the Purchasing Office shall execute the Agreement which shall include a privacy clause requiring the third party to implement appropriate measures to safeguard the confidential information, to refrain from sharing any such information with any other party, and obtain evidence that CSU minimum insurance requirements have been met.

In addition to the CSU insurance requirements for service agreements, third-party agreements/confidential information shall include the requirement that the third party be bonded and maintain commercial general liability insurance or a program of cyber risk insurance which protects against allegations of violation of privacy rights of individuals as a result of misuse, theft, or improper or insufficient care of confidential information on the part of the third party. The third party shall provide to the University documentation including Certificates of Insurance that evidence these requirements.

**FURTHER INFORMATION**

Information Security Management and Compliance  
iso@csulb.edu.  
(562) 985-2283