



CALIFORNIA STATE UNIVERSITY, LONG BEACH

Subject: Requirements for Service Providers – Access to Personal Information	
Department: Information Security Management and Compliance	Reference No.:
Division: Administration and Finance	Issue Date: April 2007
References: • Gramm-Leach-Bliley Act; FTC-15USC Subchapter I, §6801-6809 & Subchapter II, §6821-6827	Revision Date: N/A
Web Links: • http://daf.csulb.edu/offices/vp/information_security	Expiration Date: N/A

I. BACKGROUND

Federal legislation designed to ensure the privacy and safeguarding of non-public personal information places specific requirements on the University when the University engages the services of service providers who in the course of providing such service will have access to the non-public personal information of CSULB faculty, staff, students and customers. Service providers may include those who store or destroy personal information; conduct forensic investigation of electronic data; or other electronic communication services.

II. STANDARD

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

III. PROCEDURES

The following requirements govern Agreements with third-party service providers in those instances where the service provider may have access to personal information:

- A. Prior to the University entering into contractual agreement with a service provider, the Purchasing Office shall determine the adequacy of the service provider's system of safeguarding information. Depending on the service to be provided, the University may consider reviewing the service provider'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 service providers system of safeguarding information has been determined to be adequate, the Purchasing Office shall execute the Agreement which shall include a privacy clause which requires the service provider to implement appropriate measures to safeguard the personal information and to refrain from sharing any such information with any other party.

In addition to the CSU insurance requirements for service agreements, Agreements shall include the requirements that the service provider be bonded and maintain personal liability insurance which protects against allegations of violations of privacy rights of individuals as a result of improper or insufficient care on the part of the service provider. The service provider 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