CALIFORNIA STATE UNIVERSITY, LONG BEACH

Subject: **Security Breach Procedures and Protocols**	
Department: **Information Security / Safety & Risk Management**	Reference No.:
Division: **Administration & Finance**	Issue Date: **June 2005**
References: **Information Security Bulletin (ISB) 2005-04**	Revision Date: **NA**
Web Links: **Security Breach Notification Plan** **CSULB Information Security**	Expiration Date: **NA**

CSU Long Beach and CSU Long Beach auxiliary organizations have the responsibility to maintain the confidentiality of information in their possession and to safeguard that information from unauthorized acquisition. Among the types of information that is maintained, *confidential information* is by far the most encompassing.

Confidential Information is information that identifies or describes an individual, including, but not limited to, his or her social security number, physical description, home address, home telephone number, ethnicity, gender, telephone number, signature, passport number, bank account number, education, financial matters, medical or employment history, and performance appraisals. It is the unauthorized acquisition of confidential information that places faculty, staff, and students at risk of being victims of identify theft.

In an attempt to stem the growth of identity theft, the State of California enacted the California Security Breach Notification Act which mandates the public disclosure of computer security breaches in which confidential information of any California resident may have been acquired, or reasonably believed to have been acquired, by an unauthorized person. Although the definition of confidential information contained in various pieces of legislation is very broad, the definition of *confidential information* as used in the California Security Breach Notification Act is quite narrow.

Under this act, *confidential information* means an individual's first name or initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number or last 4 digits of SSN with date of birth (DOB);

(2) Driver's license number or California Identification Card number;

(3)Account number (including student identification number), credit of debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Any CSULB of CSULB auxiliary organization employee who believes that a security breach has occurred shall immediately notify the Vice President, Administration and Finance and the Information Security Officer, 985-8260. After business hours, notification shall be made to University Police, 985-4101.

The campus *Security Breach Notification Plan*, containing campus procedures and protocols to be followed in the event of a security breach can be accessed at: http://daf.cuslb.edu/offices/vp/information_security/index.html.

For further information, contact the campus Information Security Officer at 985-8260.

FORMS: NA