



# CALIFORNIA STATE UNIVERSITY, LONG BEACH

Subject: <b>Security Incident Reporting and Breach Notification Procedures</b>	
Department: <b>Information Security Management and Compliance</b>	Reference No.:
Division: <b>Administration and Finance</b>	Issue Date: <b>June 2005</b>
References: <b>• California Civil Code Sections 1798.29 and 1798.82</b>	Revision Date: <b>January 2009</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>

This document outlines procedures and protocols for notification of and response to a security breach involving unencrypted electronic personal information processed and/or maintained by the university and its auxiliary organizations.

## I. SECURITY INCIDENT REPORTING & INVESTIGATION PROTOCOL

### A. Security Incident Reporting

Any employee or data owner who believes that a security incident has occurred, shall immediately notify the Vice President, Administration and Finance and the Information Security Officer. After business hours, notification shall be made to University Police (562) 985-4101.

Upon notification by an employee, Information Technology Services, or University Police of a suspected unauthorized acquisition of confidential information the Information Security Officer, or the Assistant Information Security Officer, shall promptly notify with the *Security Breach Response Planning Group*.

### B. Security Incident Investigation

The Information Security Officer and/or the Assistant Information Security Officer will conduct an investigation into the security incident to determine whether there has been a security breach. As part of the investigation, and when applicable, the appropriate administrator shall require the data owner to complete and submit an *Employee Identification of Stored Data* statement to the Information Security Officer or Assistant Information Security Officer. All investigatory work will be documented within an *Incident Report*.

Upon completion of the investigation, the Information Security Officer or the Assistant Information Security Officer will inform the *Security Breach Response Planning Group* of the result of the investigation.

## II. SECURITY BREACH NOTIFICATION PROTOCOL

### A. Internal Notifications

If it is determined after investigation that a security breach involving notice triggering information has occurred, the Information Security Officer shall notify the Vice President of Administration and Finance and Office of General Counsel.

If it is determined that a breach is of the appropriate magnitude and may require a press release, the Information Security Officer shall notify the Senior Director, Information Security Management, Associate Vice President, University Relations, Office of the Chancellor and copy the CIO/Assistant Vice Chancellor.

The Information Security Officer or Assistant Information Security Officer will notify the responsible department, confirming the security breach of notice triggering information and provide advice and guidance. The Information Security Officer or Assistant Information Security Officer shall also initiate the campus breach notification process and work closely with the Division Executive or designee of the department responsible for controlling access to, and security of, the breached electronic equipment to ensure the appropriate handling of the breach response and inquiries. The Information Security Officer or Assistant Information Security Officer will provide guidance to designated employees responsible for responding to breach notification inquiries.

## **B. External Notification**

If it is determined after investigation that a security breach involving credit/debit card information has occurred, the Information Security Officer will direct notification to the appropriate merchant bank(s). Within three (3) business days of a confirmed breach, the Information Security Officer shall provide an Incident Report to the appropriate merchant bank(s). Within ten (10) business days, the Information Security Officer shall provide to the appropriate merchant bank(s) a list of all potentially compromised accounts.

## **C. Notification of Affected Individuals**

The department or office responsible for controlling access to, and security of, the breached electronic equipment shall compile the list of the names of persons whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In consultation with the Information Security Officer or the Assistant Information Security Officer, a list of individuals to notify shall be compiled based on the following criteria:

- Residents of California.
- All individuals who are likely to have been affected, such as all whose information had been stored in the files involved, when identification of specific individuals cannot be made.

If notices are sent to more than 10,000 individuals, the Information Security Officer or the Assistant Information Security Officer shall notify the following consumer credit reporting agencies:

- **Experian:** E-mail to [BusinessRecordsVictimAssistance@experian.com](mailto:BusinessRecordsVictimAssistance@experian.com)
- **Equifax:** E-mail to [lanette.fullwood@equifax.com](mailto:lanette.fullwood@equifax.com)
- **TransUnion:** E-mail to [fvad@transunion.com](mailto:fvad@transunion.com), with "Database Compromise" as subject.

The process for determining inclusion in the notification group shall be included in the *Incident Report*.

## **D. Notification Timing**

Individuals whose notice-triggering information has been compromised shall be notified in the most expedient time possible, and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

The information considered when determining the notification date shall be included within the *Incident Report*.

## **E. Content of Notice**

The breach notification will provide a brief description of the security breach, a contact for inquiries, and helpful references to individuals regarding identity theft and fraud. The content of the breach notification, and when appropriate, the content of both the web site page and the press release will be reviewed and approved by the Information Security Officer or Assistant Information Security Officer.

## **F. Communications with Outside Agencies**

With the exception of the Office of Public Affairs, University Police, and Safety, Risk Management & Information Security, university personnel are not authorized to speak on behalf of the university to media personnel or representatives of other outside agencies. All media inquiries or other public affairs inquiries should be directed to the Office of Public Affairs at (562) 985-4134. All other inquiries should be directed to Safety, Risk Management & Information Security at (562) 985-4862 or to the University Police at (562) 985-4101.

## **G. Method of Notification**

A letter shall be printed with official California State University, Long Beach letterhead, addressed to the individual at the last recorded home address, or if only an email address is known, the last recorded email address with the University. Any notices returned with address forwarding information will be re-sent by the responsible department.

If less than 500,000 individuals were affected, or if the cost of disseminating individual notices is less than \$250,000, notices shall be sent by first class mail or email address.

If more than 500,000 individuals were affected or if the cost of giving individual notices to affected individuals is greater than \$250,000 or if there is insufficient contact information, the following substitute notification procedures shall be followed:

- Notices by e-mail shall be sent to all affected individuals whose e-mails are known.
- The University shall issue a press release to the media as appropriate.
- A "Notice of Breach" shall be conspicuously posted on the campus web site\*.

\*After a six month period of time the Office of General Council, Associate Vice President, University Relations, and the Information Security Officer will determine if additional website posting time is necessary.

## **H. Breach Notification Inquiry Response**

Subsequent to a security breach notification, the University can expect several inquiries from notified users, their parents/spouse, and security vendors. The Information Security Officer or the Assistant Information Security Officer will provide a written *Inquiry Response Guide* to be used by the Division Executive, or designee(s), to respond to any phone calls/emails/letters/walk in traffic with inquiries regarding the breach.

## **I. Department Responsibility**

The department responsible for controlling access to, and security of, the breached electronic information is responsible for financial and human resources used to notify and respond to the affected individuals.

### III. DEFINITIONS

<b>Confidential Information</b>	Confidential Information is information that identifies or describes an individual. Confidential Information is further detailed in the <a href="#">CSULB Information Security and Privacy Program</a> .
<b>Data Acquisition</b>	<p>Unencrypted electronic personal information/notice-triggering information will be considered to have been acquired, or reasonably believed to have been acquired, by an unauthorized person in any of the following situations.</p> <ol style="list-style-type: none"><li>1. <b>Equipment</b> – Lost or stolen electronic equipment (including palm pilots, laptops, desktop computers, and USB storage devices) containing unencrypted personal information.</li><li>2. <b>Hacking</b> – A successful intrusion of computer systems via the network where it is indicated that unencrypted personal information has been downloaded, copied, or otherwise accessed</li><li>3. <b>Unauthorized Data Access</b> – Includes situations where someone has received unauthorized access to data, such as sending non public mail/e-mail to the wrong recipient, incorrect computer access settings, inadvertent posting of personal information in electronic format or other non-hacking incidents. Unauthorized data access also includes indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.</li></ol>
<b>Data Owner</b>	The individual with primary responsibility for determining the purpose and function of a record system.
<b>Encryption</b>	All encryption algorithms, with the exception of trivial ciphers, meet the minimal campus requirements for encryption. If personal information stored on the compromised electronic equipment is encrypted, no University notification is required.
<b>Health Insurance Information</b>	An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.
<b>Incident Report</b>	An investigatory summation of a <u>Security Incident</u> completed by the <u>Information Security Officer</u> or the <u>Assistant Information Security Officer</u> to determine if the university has incurred a <u>Security Breach</u> .
<b>Medical Information</b>	Information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.
<b>Notice-Triggering Information</b>	Specific items of personal information identified in CA Civil Code Sections 1798.29 and 1798.3. This information includes an individual's name in combination with Social Security Number, driver's license/California identification card number, health insurance information, medical information, or financial account number such as credit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

<b>Security Breach</b>	An unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information maintained by California State University, Long Beach or its auxiliary organizations.
<b>Security Breach Response Planning Group</b>	Individuals designated by the University to address Information Security issues. The group includes the Associate Vice President/Dean of Students, Student Services, Associate Vice President of Academic Technology, Associate Vice President, Information Technology Services, Associate Vice President, University Relations, Associate Vice President, Academic Technology, Technology Strategist, Information Security Officer, Assistant Information Security Officer, and the Chief of Police.
<b>Security Incident</b>	A collection of related activities or events which provide evidence that confidential information could have been acquired by an unauthorized person.

#### **IV. LEGAL OR CIVIL ACTIONS**

Subsequent to a breach, the University may be reviewed by a governing state or federal agency or a civil action could be brought against the University. The University office of Information Security Management and Compliance will represent all complaints and agency inquiries submitted to the University as a result of the security breach. Legal counsel will be solicited as needed to respond to complaints or actions. The University is responsible for the payment of fines, penalties, or retributions levied by agencies or the courts.

#### **FURTHER INFORMATION**

Information Security Management and Compliance  
 iso@csulb.edu.  
 (562) 985-4862