



CALIFORNIA STATE UNIVERSITY, LONG BEACH

Subject: Protecting the Confidentiality of Social Security Numbers	
Department: Information Security Management and Compliance	Reference No.:
Division: Administration and Finance	Issue Date: June 2005
References: <ul style="list-style-type: none"> • CSU HR 2005-07, Legislation Change Regarding use of Social Security Numbers • California Civil Code, Section 1798.85-1798.86 • California Labor Code, Section 226 	Revision Date: April 2008
Web Links: <ul style="list-style-type: none"> • http://daf.csulb.edu/offices/vp/information_security 	Expiration Date: N/A

I. BACKGROUND

The Social Security Number (SSN) has a unique status as a privacy risk. No other form of personal identification plays such a significant role in linking records that contain sensitive information that individuals generally wish to keep confidential. The broad use and public exposure of SSNs has been a major contributor to the tremendous growth in recent years in identity theft and other forms of credit fraud. The need to significantly reduce the risks to individuals of the inappropriate disclosure and misuse of SSNs has led California to enact legislation to limit their use and display. California law is intended to deter public disclosure of social security numbers. It does not prohibit use of social security numbers for internal verification, or administrative purpose, or as otherwise required by law.

II. PROHIBITED USE OF SOCIAL SECURITY NUMBERS (SSN)

In compliance with California Civil Code Sections 1798.85-1798.86 and California Labor Code Section 226 California State University, Long Beach (CSULB) and CSULB auxiliary organizations are prohibited from doing any of the following:

- Publicly posting or displaying an individual's SSN;
- Printing an individual's SSN on identification cards or badges;
- Requiring persons to transmit a SSN over the Internet unless the connection is secure or the number is encrypted;
- Requiring persons to log onto a web site using a SSN without a password;
- Printing SSNs on anything mailed to an individual unless required by law or the document is a form or application. When sending applications, forms, or other documents required by law to carry SSNs through the mail, the SSN shall be placed where it will not be revealed by an envelope window. SSNs may not be printed on a postcard;
- Encoding or embedding a SSN in a card or document, including using a bar code, chip, magnetic strip, or any other technology;
- Printing more than the last four digits of an employee's SSN on employee pay stubs or itemized statements.

III. STANDARD

In addition to complying with the legal requirements concerning the use and display of SSNs, CSULB and CSULB auxiliary organizations shall take the following measures to reduce the collection of SSNs, control access to SSNs, and protect SSNs with security safeguards:

Reduce the Collection of SSNs

- Collect SSNs preferably only where required to do so by federal or state law.
- When collecting SSNs as allowed, but not required, do so only as reasonably necessary for the proper administration of lawful business activities.
- If a unique personal identifier is needed, use employee or student identification number, or develop a substitute for the SSN.

Control Access to SSNs

- Limit access to records containing SSNs only to those who need to see the numbers for the performance of their duties.
- Protect records containing SSNs, including back-ups, during storage by encrypting the numbers in electronic records or storing records in other media in locked cabinets.
- Do not store records containing SSNs on computers or other electronic devices that are not secured against unauthorized access.
- Do not share SSNs with other organizations or persons except where required by law.
- Prohibit third parties from using SSNs, except as required by law.

Protect SSNs with Security Safeguards

- Comply fully with the CSULB Clean Desk and Clear Screen Standard.
- Do not leave voice mail messages containing SSNs .
- Do not fax documents containing SSNs to public FAX machines.
- Promptly report any inappropriate disclosure or loss of records contains SSNs to your supervisor and the campus office of Information Security Management and Compliance. See **Security Incident Reporting and Breach Notification Procedures**.
- Discarding or destroying documents containing SSN must be accomplished in accordance with the campus Media Sanitization Standard.

FURTHER INFORMATION

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