User Guidelines for Reporting a Lost or Stolen Computer or Electronic Storage Device				
	Number	ITS-1008-G	Rev:	--
	Owner:	IT Security Management and Compliance		
	Approved by:	Bev Mitchum Director, IT Security and Compliance		
	Issued:	5/2/05	Effective:	5/2/05
				Page 1 of 3

1 Purpose

California State Senate Bill (SB) 1386, effective July 1, 2003, regulates the maintenance and dissemination of personal information by state agencies, and requires each agency to keep an accurate account of disclosures of personal information. This bill requires all organizations electronically storing personal information on California residents to notify residents if their information is unencrypted and is accessed by someone unauthorized to do so. Other Federal and State laws and regulations also govern the handling, storage, and dissemination of confidential information.

These guidelines apply to users of campus desktop computers, laptops, and electronic storage devices, as well as to owners of desktop computers, laptops, and storage devices that contain University data, including personal, confidential, and/or proprietary information. These guidelines outline the steps users must take to ensure the campus complies with all law and regulations regarding personal and confidential information when desktop or laptop computers and electronic storage devices are lost or stolen.

2 Definitions

Confidential Information
In addition to those listed in the Personal Information definition below: financial records; medical records; physical description; home address; home phone number; education; grades; ethnicity; gender; employment history; performance evaluations; disciplinary action plans; NCAA standings; etc. Confidential information must be interpreted in combination with all information contained on the computer to determine whether a violation has occurred.

Personal Information under SB 1386
The individual's first name or first initial and last name in combination with any one of the following: Social Security Number (SSN); driver's license number; California Identification Card; account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Proprietary Information
Information that an individual or entity possesses, owns, or holds exclusive rights to. Examples include: white papers; research papers; business continuity and other business operating plans; e-mail messages; vitae; letters; confidential business documents; participants of an organization, class, or group; detailed building drawings; network architecture diagrams; etc. Proprietary information, if lost or stolen, could compromise, disclose, or interrupt operations or embarrass the individual or the university.

3 Related Documents

The following documents, forms, and logs of the latest issue in effect shall apply to the extent specified herein.

ID/Control #	Title
ITS-2804	Lost or Stolen Computer or Electronic Storage Device Report

4 Guidelines

a) The reporting party should contact University Police ***immediately***.
Telephone: (323) 343-3700
Location: Department of Public Safety, Building C

b) The reporting party should ***immediately*** complete the *Lost or Stolen Computer or Electronic Storage Device Report* form. Include the reporting officer's name and the University Police report number (this information will be provided by the reporting officer.)

NOTE

The reporting party may obtain a hardcopy of the form from University Police, or download an electronic copy from the Information Technology Services (ITS) Forms website: www.calstatela.edu/its/forms (look under the Incident Response topic). If downloading the form from the website, first save the form to the hard disk, open the form within the application (usually Microsoft Word), complete the form, save the completed form to the hard disk, and attach this saved version to the e-mail message.

c) The reporting party should submit the completed *Lost or Stolen Computer or Electronic Storage Device Report* form

Take hardcopy to LIB PW 1070, or
E-mail electronic form to ITSecurity@calstatela.edu.

d) University Police reporting officer will e-mail ITSecurity@calstatela.edu the following information:

Computer Theft Location
Report Number
Reporting Party
Reporting Officer

NOTE

If the reporting party refuses to complete the *Lost or Stolen Computer or Electronic Storage Device Report* form, the reporting officer shall include this language in the e-mail message: **"Reporting party REFUSED to complete the stolen computer or electronic storage device report."**

e) After IT Security Management and Compliance receives *Lost or Stolen Computer or Electronic Storage Device Report* form, it will:

- Complete the Office Use Only section on the form, including the IT Security Case Number.
- Print a copy and forward it to:
  Department of Public Safety, Building C
  Attn: Police Records
- If the lost or stolen equipment contains confidential, personal, and/or proprietary information, IT Security Management and Compliance must also forward a copy of the completed report form to the University Counsel, who will coordinate further action with the reporting department.

f) If the lost or stolen equipment contains confidential, personal, and/or proprietary information, the responsibility for notifying victims under SB 1386 resides with the department or division where the security breach occurred.

5 Terms, Conditions, and/or Sanctions

This section is not applicable to the herein guidelines.

6 Contacts

To report lost or stolen computers and/or electronic storage devices, contact:

University Police (323) 343-3700
Department of Public Safety, Building C

For questions regarding this procedure, contact:

IT Security Management and Compliance (323) 343-2600
Information Technology Services, LIB PW 1070
ITSecurity@calstatela.edu