 <b>User Guidelines for Laptop Security</b>	Guidelines No.	ITS-1007-G	Rev:	B
	Owner:	IT Security Management and Compliance		
	Approved by:	Peter Quan, VP ITS and CTO		
	Issued:	5/12/06	Effective:	5/12/06
	Page 1 of 6			

## 1 Purpose

Laptops require even greater security precautions against theft and confidentiality breaches than desktop computers. While portability makes laptops exceptionally convenient, it also makes them more vulnerable to physical damage, theft, and information security breaches. If the wireless function is enabled without applying security measures, a personal firewall, and anti-virus software, the laptop may be vulnerable to intrusions and/or viruses. Because laptops are so portable, they generally operate outside and beyond the campus Information Technology Services (ITS)-managed firewalls and layered virus/intrusion protection. In addition, California Senate Bill 1386 (SB 1386), effective July 2003, makes it mandatory for the campus to notify all victims of their potential identity theft whenever an event occurs during which there is a loss or possible loss of confidential data. If a laptop is stolen or otherwise compromised, the responsibility for notifying victims under SB 1386 resides with the department or division where the security breach occurred. Therefore, faculty and staff members using a Cal State L.A. (herein "University") laptop computer or their own laptop containing confidential University data assume responsibilities beyond those of a campus desktop computer user.

This procedure outlines the steps for securing laptops and the personal, confidential, and/or proprietary information contained on them.

## 2 Definitions

### Anti-Virus Software

Programs to detect and remove computer viruses. The simplest anti-virus programs scan executable files and boot blocks for a list of known viruses. Others are constantly active, attempting to detect the actions of general classes of viruses. Anti-virus software should always include a regular update service that downloads the latest virus definitions and "inoculations."

### 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.

### Dynamic Host Configuration Protocol (DHCP)


A protocol for assigning dynamic IP addresses to devices on a network.

### Firewall

A system designed to prevent unauthorized access to or from a private network or an individual computer. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks, especially intranets, connected to the Internet. When a firewall is "up" (i.e., active), it examines all messages passing through it (i.e., entering or leaving a private network), and blocks those that do not meet the specified security criteria.

### Internet Message Access Protocol (IMAP)

A protocol for retrieving e-mail messages. IMAP 4 is similar to pop3 but supports some additional features.

 <b>User Guidelines for Laptop Security</b>	Guidelines No.	ITS-1007-G	Rev:	B
	Owner:	IT Security Management and Compliance		
	Approved by:	Peter Quan, VP ITS and CTO		
	Issued:	5/12/06	Effective:	5/12/06
	Page 2 of 6			

Laptop Cable

A cable secured to the laptop and an immovable object, so used to prevent the theft of the laptop. Generally use combination locks.

Media Access Control (MAC) Address Control

A Media Access Control (MAC) address is a unique identification serial number (also known as the physical address, Ethernet address, adaptor address, or hardware address) on a computer's network card that identifies this computer on a network. When MAC addresses are registered on the computer's wireless card, that computer should only "talk" to those registered to it. Using MAC address control is not a guarantee of full security because MAC addresses can be copied (i.e., "spoofed"). However, it does make it more difficult for others to make unauthorized access.

Network Router

A device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network. Routers are located at gateways, the places where two or more networks connect.

Operating System (OS)

Software designed to control hardware of a specific data-processing system in order to allow users and applications to make use of it.

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.

Secure Shell (SSH)

A program used to log into another computer over a network. SSH provides strong authentication and secure communications over insecure channels.

Secure Sockets Layer (SSL)

A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a private key to encrypt data that's transferred over the SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many websites use the protocol to obtain sensitive information such as credit card numbers. By convention URLs that require an SSL connection start with "https" instead of "http."

 <b>User Guidelines for Laptop Security</b>	Guidelines No.	ITS-1007-G	Rev:	B
	Owner:	IT Security Management and Compliance		
	Approved by:	Peter Quan, VP ITS and CTO		
	Issued:	5/12/06	Effective:	5/12/06
Page 3 of 6				

### Security Breach

Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained on it.

### Service Set Identifier (SSID)

The wireless network name. A 32-character unique identifier attached to the header of packets sent over a wireless LAN. SSIDs act as a password when a mobile device tries to connect to a 802.11b network. The SSID differentiates one wireless LAN from another. All access points and devices attempting to connect to a specific wireless LAN must use the same SSID. An SSID does not provide any security to the network.

### Virtual Private Network (VPN)

VPN software allows a secure, encrypted connection to be made with another machine or network. The University provides a Cisco VPN client for this purpose.

### Wired Equivalent Privacy (WEP)

A security protocol for wireless local area networks. WEP is designed to provide the same level of security as that of a wired LAN, providing security to protect transmitted data by encrypting it over radio waves.

### Wireless Access Point (WAP)

Distinctively configured nodes on wireless local area networks (WLANs) that act as central transmitters and receivers of WLAN radio signals.

### Wi-fi Protected Access (WPA)

A wi-fi standard designed to improve upon the security features of WEP.

## 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
ITS-1008-G	User Guidelines for Reporting a Lost or Stolen Computer or Electronic Storage Device

## 4 Guidelines

Laptop security measures and safeguards are outlined in the following sections. For more detailed information and tips on laptop security, visit the campus Are You **Secure?** website at <http://www.calstatela.edu/itsecurity>.

### 4.1 Implement Security Measures for New or First-Issued Laptops

- a) Departments and users/owners should keep all laptop identifying information (make, model, serial number, and inventory number (if any)), as well as emergency telephone

 <b>User Guidelines for Laptop Security</b>	Guidelines No.	ITS-1007-G	Rev:	B
	Owner:	IT Security Management and Compliance		
	Approved by:	Peter Quan, VP ITS and CTO		
	Issued:	5/12/06	Effective:	5/12/06
	Page 4 of 6			

numbers used to report a loss or theft (see Section 4.5) in a safe, accessible location, but not with the laptop.

- b) Configure the laptop's security settings for optimal security. Install, run, and regularly update anti-virus software. Disable the guest account feature and all auto-login and save password functions. Prevent user names from being displayed at log in and do not load passwords on the laptop. For regular use, do not use the Administrator account. Use strong passwords and authenticate access where possible.


## 4.2 Safeguard Laptop Contents

- a) Install software only from known, legitimate sources, and never let unauthorized users install or download anything to your laptop. Keep your business laptop for business purposes, and do not let anyone else use it. Prevent others from seeing the screen or watching you type while typing in a password or working on confidential or sensitive material.
- b) Regularly update operating system and application patches and services packs.
- c) Keep confidential and sensitive information on a removable drive or device, and do not store this with the laptop. Encrypt data files, especially those containing confidential, personal, and/or proprietary information. Back up all data files regularly, especially before traveling. Consider installing software that conceals your laptop's hard drive information.
- d) Use a surge protector and consider using an anti-theft locator device.
- e) Properly log off websites before closing the browser, and delete cookies, files, temporary cache, and history.

## 4.3 Secure the Wireless Laptop Connection

Wireless networks use radio frequencies to transmit and receive data, making them vulnerable to others easily tapping into an unsecured wireless connection without the user's knowledge. Such intruders can send messages and gain unauthorized access to other wireless networks and transmissions as well. This is one of the methods employed by thieves to obtain the information needed for identity theft. Laptop users should use all available security features and tools to prevent unauthorized use of their computers. See <http://www.calstatela.edu/itsecurity> for more detailed information.

- a) Use a network address translation (NAT) router to close off access. Disable the wireless card and WAP address when not in use.
- b) Use the latest wireless security standard (WPA), or transmit data using WEP with a strong key. Use MAC address control, which should ensure that only addresses registered to the wireless card can communicate with it. Change the default service set identifier (SSID), i.e., the wireless network name, to one that is difficult to guess. Prohibit the broadcast of the SSID so that it does not indicate its availability for use. If possible, change the WAP's default channel addresses and set the WAP to receive, but not to broadcast. Disable DHCP or change the default address range.

 <b>User Guidelines for Laptop Security</b>	Guidelines No.	ITS-1007-G	Rev:	B
	Owner:	IT Security Management and Compliance		
	Approved by:	Peter Quan, VP ITS and CTO		
	Issued:	5/12/06	Effective:	5/12/06
Page 5 of 6				


- c) Install and use a personal firewall.
- d) Use an encrypted VPN connection when accessing University resources. This requires that the laptop have a network card. VPN software for faculty and staff is available for downloading at <http://www.calstatela.edu/its/techsupport/softapp/>. [Note: GET and GETLA are secure websites (using https://), and, therefore, do not require VPN access.]
- e) Always encrypt confidential or sensitive data when transmitting from a wireless laptop.
- f) Turn off file sharing and do not use unencrypted instant messaging (IM).
- g) Use SSL or SSH for any transmission requiring a password. Use secure e-mail protocols.

#### 4.4 Physically Safeguard the Laptop

- a) Treat the laptop like you would a wallet or purse containing money and personal information. Do not carry the laptop in a case behind you; otherwise thieves can unzip or unbuckle the case and take off with the laptop before you realize it's gone.
- b) Keep the laptop in your possession at all times. Never leave the laptop unattended, even in your office or for a few seconds. If you have to put it down, put it on your lap or between your feet. Never ask others, especially strangers, to watch the laptop for you. In an office, secure the laptop with a separate laptop cable locking device, preferably one with an alarm, and lock it in a file cabinet or desk drawer when leaving the office for the day. Never place the laptop where it can fall or be run over.
- c) If allowed, put a distinctive marking on the laptop. Since thieves are on the lookout for laptop carrying cases, store the laptop in a case that doesn't look like a standard case.
- d) Never leave the laptop visible in a car or near an exterior window. If you must leave the laptop in a car, lock the laptop in the car trunk, making certain no one sees you doing so.
- e) Be especially cautious in certain locations where theft might likely occur, such as public transportation and depots, offices, conferences, restaurants, hotels, college campuses, phone booths, libraries, and hospitals. Do not leave the laptop in a hotel room. Keep an eye on the laptop at security checkpoint conveyor belts.
- f) Never check the laptop at airports; carry it on the plane with you. Never put the laptop in overhead storage bins on planes, buses, or trains. Never store the laptop in an airport, bus, or train station locker.
- g) Prepare the laptop for security checkpoints. Be aware of restrictions when you travel abroad.

#### 4.5 Report Laptop Damage, Loss, Theft, and Security Breach Immediately

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

 <b>User Guidelines for Laptop Security</b>	Guidelines No.	ITS-1007-G	Rev:	B
	Owner:	IT Security Management and Compliance		
	Approved by:	Peter Quan, VP ITS and CTO		
	Issued:	5/12/06	Effective:	5/12/06
	Page 6 of 6			

- 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](http://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 forward the completed *Lost or Stolen Computer or Electronic Storage Device Report* form immediately: Either:

Take hardcopy to LIB PW 1070, or  
E-mail electronic form to [ITSecurity@calstatela.edu](mailto:ITSecurity@calstatela.edu).

## 5 Terms, Conditions, and/or Sanctions

This section is not applicable to the herein guidelines.

## 6 Contacts

- a) To report a lost or stolen laptop, contact University Police at (323) 343-3700.
- b) To report a security breach, contact the University Counsel at (323) 343- 5105.
- c) For questions regarding general information technology security, contact IT Security Management and Compliance at [ITSecurity@calstatela.edu](mailto:ITSecurity@calstatela.edu).
- d) For technical assistance contact the ITS Help Desk at 3-6170.
- e) For questions regarding specific department procedures, contact the department administrator.