User Guidelines for Mobile Computing	Guideline No.	ITS-1020-G	Rev:	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director IT Security and Compliance		
	Issued:	2-15-12	Effective:	2-15-12
				Page 1 of 13

Table of Contents

1 Purpose....2
2 Entities Affected by This Guideline....2
3 Definitions....2
4 Guidelines....3
4.1 Employee Usage of Mobile Computing Devices....4
4.2 Protected Data....4
4.3 Physical Security....4
4.4 Preventing Unauthorized Access....5
4.4.1 Mobile Electronic Devices....5
4.4.2 Operating Systems....5
4.4.3 Wireless Access....6
4.4.4 Cellular and Removable Media Devices....6
4.5 Off-campus Computing Equipment Use....6
4.6 Documentation....6
4.7 Official Travel with Mobile Computing Devices....7
4.8 Out of Country Travel with Mobile Computing Devices....8
4.9 Inventory of Mobile Computing Devices....9
4.10 Reporting....9
5 Contacts....10
6 Applicable Federal and State Laws and Regulations....10
7 Related Documents....11

1 Purpose

With advances in computer technology, mobile computing becomes a useful tool to meet the business needs at CSULA. Mobile computing devices can be expensive, highly functional, easily portable and in great demand and, therefore, are especially susceptible to loss, theft and hacking. The features that make mobile computing useful (portability, access connectivity, data storage, processing power) also make them a security risk to users and to CSULA when these devices contain protected University data.

The purpose of this guideline is to establish an authorized method for controlling mobile computing devices that contain or access CSULA protected data. These following guidelines are necessary to preserve the integrity, availability and confidentiality of this data. This guideline applies to any device used to access or store protected CSULA data including both institutional and privately owned/funded devices.

2 Entities Affected by This Guideline

This guideline applies to all University employees.

3 Definitions

a) 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."

b) Encryption: A procedure used to convert data from its original form to a format that is unreadable or unusable to anyone without the tools/information needed to reverse the encryption process.

c) 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.

d) Level 1 Confidential Data: Confidential data is information maintained by the University that is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws. Its unauthorized use, access, disclosure, acquisition, modification, loss or deletion could result in severe damage to the CSU, its students, employees or customers. Financial loss, damage to the CSU's reputation and legal action could occur if data is lost, stolen, unlawfully shared or otherwise compromised. Level 1 data is intended solely for use within the CSU and limited to those with a "business need-to-know." Statutes, regulations, other legal obligations or mandates protect much of this information. Disclosure of Level 1 information to persons outside of the University is governed by specific standards and controls designed to protect the information.

e) Level 2 Internal Use Data: Internal use data is information that must be protected due to proprietary, ethical or privacy considerations. Although not specifically protected by statute, regulations or other legal obligations or mandates, unauthorized use, access, disclosure, acquisition, modification, loss or deletion of information at this level could cause financial loss, damage to the CSU's reputation, violate an individual's privacy rights or make legal action necessary. Non-directory educational information may not be released except under certain prescribed conditions.

f) Malware: Software of malicious intent/impact such as viruses, worms and Spyware.

g) Mobile Computing Device: A portable device such as a laptop, tablet PC, Personal Digital Assistant (PDA) or cell phone with computer functions that are capable of storing, processing, displaying and communicating data and is equipped with wireless or wired communication capability.

h) Network Address Translation (NAT): A process of modifying network address information in packet headers while in transit across a traffic routing device. NAT readdresses outbound packets to mask the internal IP addresses of the network. NAT allows the University to hide the topology and address schemes of its trusted network from untrusted networks.

i) Operating System: Software designed to control hardware of a specific data processing system in order to allow users and applications to make use of it.

j) Personal IT Resources: Computing and communications devices owned by the employee that may be used for University business. Examples include home computers, personal laptops, personal PDAs or cell phones and personal electronic storage devices.

k) Protected Data: An all-encompassing term that includes any information defined herein as confidential, personal, proprietary, health insurance or medical information. See Level 1 Confidential Data and Level 2 Internal Use Data.

l) Security Breach: Unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information maintained on it.

m) Wi-Fi Protected Access 2 (WPA2): Security protocol for wireless local area networks that indicates a product has successfully completed testing under the Wi-Fi Alliance's Wi-Fi Protected Access 2 certification program and meets the criteria established to ensure stronger data protection for multiple users and large managed networks. These criteria prevent unauthorized network access by verifying network users through an authentication server.

4 Guidelines

The most effective way to secure protected data is not to store it on a mobile computing device. A second secure technique is to keep protected data only on secure central University servers and access it remotely using secure communication techniques outlined in this guideline. However, University business requirements may on occasion justify storing protected data on a mobile computing device. In those limited cases, users are required to observe this guideline to ensure that all possible steps have been taken to keep the University's protected data secure. These guidelines are applicable to mobile computing devices no matter their location (e.g., travel, at home, etc.).

4.1 Employee Usage of Mobile Computing Devices

All University employees are:

- Prohibited from using University-provided portable devices for personal business, except for incidental and minimal personal use as provided by Government Code 8314.
- Personally responsible for updating anti-virus software, security patches and operating system upgrades on any and all devices being used for University business (see 4.2 below).
- To return equipment on due date, upon request or upon termination of employment.
- To immediately report stolen or missing on-campus equipment to University Police or off-campus equipment to the nearest law enforcement agency, and provide the related Incident/Case # on form *ITS-2804 Lost/Stolen Computer/Electronic Storage Device Report.*
- Responsible for ensuring that University mobile computing devices and accompanying data are handled as University property.

4.2 Protected Data

Storage of protected data on any mobile computing device should be avoided where possible, regardless of who owns the device.

The storage of protected data on a CSULA or non-CSULA (e.g., personal) mobile computing device is prohibited unless the criteria below are met:

- The device stores only the minimum data necessary to perform the function necessitating storage on the device.
- Information is stored only for the time needed to perform the function.
- The device on which protected data is stored is secure (e.g., it includes anti-virus software that is consistently updated; operating systems are consistently upgraded; etc.).
- Data is protected from any and all forms of unauthorized access and disclosure by encrypting the storage and transmission of protected data.
- Data is not transferred from a mobile device to any device not known to be secure.
- Data is not downloaded to a hard drive or other mobile computing device if the data is available, accessible and utilizable on other systems.

4.3 Physical Security

Users must take all reasonable and appropriate precautions to protect and control a mobile computing device used for University business. A mobile computing device shall be physically protected from unauthorized physical access, tampering, loss or theft.

- All University laptops must be registered in the CSULA asset management system.
- Keep devices with you at all times or store them in a secured location when not in use.
- Do not leave devices unattended in public locations (e.g., airport lounges, meeting rooms, restaurants, etc.).
- Users must not leave mobile computing devices in view in an unattended vehicle, even for a short period of time.
- Users must secure unattended devices in a locked cabinet or filing cabinet or in a locked private office.
- Mobile computer asset recovery software is recommended to enable authorities to locate and return the asset.

- o If allowed, put a distinctive marking on the laptop.

4.4 Preventing Unauthorized Access

4.4.1 Mobile Electronic Devices

All mobile electronic devices in which University-related protected data are stored, including laptops, smartphones and PDAs must, if applicable:

- o Configure security settings for optimum security.
- o Disable all auto-logins and save password functions.
- o Disable the guest account feature.
- o Prevent user names from being displayed at log in. Laptops should be configured to prevent the last logged-in user name from being displayed after a person logs off or when a computer is restarted.
- o Do not load passwords or PINs on the laptop. Passwords and personal identification numbers (PINs) are your keys to e-mail and other accounts.
- o Require that a strong password be provided when a user first logs in or when the system is accessed after a period of inactivity.
- o Take precautions to prevent others from observing passwords being entered.
- o The device should lock if the user password authentication fails three times.
- o Take care to securely preserve access keys and passwords to recover data. Decryption keys locked in safes, safety deposit boxes or otherwise stored in a safe location can help prevent a data loss catastrophe.
- o Users must not grant access to their mobile devices to unauthorized individuals.
- o Users may not bypass or disable security mechanisms under any circumstances.
- o Properly log off web sites before closing the browser, and delete cookies files, temporary cache and history.
- o Install software only from known, legitimate sources and never let unauthorized users install or download anything to a mobile computing device, if applicable.
- o Use the mobile computing device for business purposes only.
- o Use an encrypted VPN connection when accessing University resources that are not protected by any other encryption method. For example, VPN is not required for Outlook Web Access (OWA) access since it is already encrypted with SSL.
- o Turn off file sharing and do not use unencrypted instant messaging.
- o Use secure e-mail protocols.

4.4.2 Operating Systems

All mobile electronic devices, including laptops, smartphones, etc. that have operating systems must:

- o Keep all operating system and application updates and patches up-to-date.
- o Install, use and update regularly anti-virus software, if applicable.
- o Enable firewalls.
- o Users must take all reasonable steps to protect against the installation of unlicensed or malicious software and malware signatures must be kept up-to-date.

4.4.3 Wireless Access

Wireless networks use radio frequencies to transmit and receive data, making them vulnerable.

- Wireless access should be disabled when not in use to prevent unauthorized wireless access.
- Disable all wireless communication technologies, e.g., Bluetooth, when not in use.
- Accounts and passwords should never travel unencrypted over a wireless network.
- Use a network address translation (NAT) router to close off access.
- Use the latest wireless security standard (WPA2).
- Never send/receive protected data over a wireless link unless another more secure end-to-end (encryption) technology is also being used.

4.4.4 Cellular and Removable Media Devices

Many cellular and removable media devices are not considered secure as they traditionally do not contain options to increase their security. Security recommendations for the device should be followed to the extent that they are technologically possible as a feature of the device.

4.5 Off-campus Computing Equipment Use

University equipment may not be removed from the campus except for official use. Approval for off-campus equipment use, including laptops, must be in writing and recorded on a *Property Loan Agreement Form*. University equipment shall not be used by anyone other than the person who signed for it without a written change of accountability.

4.6 Documentation

Department and users/owners should keep the following information:

- All laptop identifying information (make, model, serial number and property inventory number, if any).
- Emergency telephone numbers used to report a loss or theft in a safe, accessible location, but not with the mobile computing device.
- If protected data is approved for storage on the mobile storage device, have written approval that it is for a legitimate business need and also a description of the data. The description of the data should include the classification of the data and be sufficient enough to allow the department to provide security breach notifications, if required, should the device be lost, stolen or the personal data otherwise unlawfully accessed or assumed to have been accessed.

4.7 Official Travel with Mobile Computing Devices

There are special security precautions when traveling with a mobile computing device that stores University-related data, whether a personal or University-issued laptop, PDA, smartphone, etc.

- Delete any information you do not need before you go.
- Make backup copies of all your important files.
- Create strong passwords for your devices and change them regularly (including when you return). Do not store the passwords anywhere.
- Avoid wireless networks and turn off ports and features you do not need.
- Install host-based protections including a personal firewall, anti-virus software and anti-spyware software.
- Apply all patches.
- Ensure that there is a required login for the operating system.
- Turn off file-sharing and print-sharing before traveling.
- Do not store any data on computers if traveling to countries with encryption restrictions. Refer to the following U.S. Department of State web pages:
  - "Tips for Traveling Abroad" (http://travel.state.gov/travel/tips/tips_1232.html)
  - "Consular Information Sheets" (http://travel.state.gov/travel/cis_pa_tw/cis/cis_1765.html)
- Only access your e-mail using a secure web client or IMAP client.
- Whenever possible, CSULA protected data should not be stored on portable computing devices. However, in the event that there is no alternative to local storage, such data must be encrypted.
  - It is recommended that if laptops store protected data that they have special laptop "tracking and recovery" software installed. This special software will track the location of a stolen laptop and can remotely delete all data on the stolen laptop's hard drive as soon as the stolen device is connected to the Internet. One popular tracking and recovery software application is Computrace, available at http://www.computrace.com. ITS began piloting the Computrace software on ITS-issued Baseline laptops in late 2009.
  - For information and assistance with purchasing or using this software on University-owned equipment, contact the ITS Help Desk.
  - ITS-managed Blackberry devices can be remotely locked, disabled or have the contents of the device completely erased.
- Protected data must not be transmitted via wireless to or from a portable computing device unless approved wireless transmission protocols and encryption techniques are utilized.
  - For technical information on currently acceptable wireless transmission protocols, visit: http://www.calstatela.edu/its/wireless/protocols/.
  - For technical information on recommended encryption tools, visit: http://www.calstatela.edu/its/desktop/encryptiontools/.
  - For assistance encrypting files, contact the information technology consultant (ITC) assigned to the department or division.
  - Document password protection is not a secure method for protecting data transmission across a wireless network.

- Be especially cautious in certain locations where theft might likely occur. Never leave your laptop out of your sight even for a moment. Busy places such as bus and train stations, airports (especially at security checkpoint conveyor belts), offices, conference and seminar centers, restaurants, hotels, college campuses, telephone booths, libraries and hospitals are places where thieves who are on the lookout for laptops easily blend into the crowd.
- Carry your laptop in a nondescript carrying case and one that does not advertise it contains a laptop.
- Do not leave your laptop in your hotel room. Leave your laptop in the hotel safe, or if that option is unavailable, leave it in your locked luggage. Beware: In some foreign countries your laptop may not be secure in the hotel safe and it may be subject to search and seizure by local intelligence or police.
- Never check your laptop at airports. Carry it on the airplane with you.
- Never put your laptop in overhead storage bins on airplanes, buses or trains.
- Never store your laptop in an airport, bus or train station locker.
- Prepare your laptop for security checkpoints. At security checkpoints in airports and elsewhere, you may have to show that your laptop is a working computer and not some other kind of device. Therefore, have the power cord with you or make sure that the battery is charged. If your laptop will not power up, you may not be permitted through the security checkpoint.

4.8 Out of Country Travel with Mobile Computing Devices

In addition to the "Official Travel with Mobile Computing Devices" information above, the following is guidance to assist employees for out-of-country travel.

United States export control laws permit employees to take "tools of the trade" (including laptops, PDAs, cell phones and digital storage devices) out of the country for up to one year. Routine uses of commercial encryption products are included in this authorization. However, just because employees can carry these items does not mean that they should.

- Be aware of restrictions when you travel abroad. Import restrictions may cause travel delays, or worse, confiscation of your laptop. Some countries ban encrypted telecommunications traffic. Know the laws and restrictions in the destination country. If you bring a new computer into the United States, you may have to pay an import tax. To prove your laptop is not new, have your laptop's sales receipt or insurance documentation with you. To avoid any confusion about your laptop's status consider registering your laptop with United States Customs before traveling.
- When traveling to foreign countries be sure to first check travel advisories from these two agencies:
  - Federal Aviation Administration (http://www.faa.gov)
  - Transportation Security Administration (http://www.tsa.gov)
- Record what equipment will be taken out of the country.
- If the laptop contains International Traffic in Arms Regulations controlled information, a license may be required.

- When an employee is stopped and questioned by an U.S. Customs and Border Patrol officer concerning their laptop or other electronic device, the employee should fully cooperate with the officer. An employee should be prepared to answer questions concerning the information contained on the device and whether the hand carried items require a license for import/export.
- The use of a laptop to transmit information through public telecommunications networks presents potential vulnerabilities due to the susceptibility to eavesdropping and interception of the information transmitted. This is especially true in overseas locations since foreign telephone systems and networks may be either owned or controlled by the host government. This allows the foreign government to easily monitor transmissions of selected U.S. corporations, government agencies and American citizens.

4.9 Inventory of Mobile Computing Devices

Administrative officials (vice presidents, deans, directors and other supervisory personnel) should maintain and update at least annually an inventory of University-provided mobile computing devices assigned to personnel within their area of supervision. The following information should be maintained; however, departments may add additional information requirements.

- Description of the item
- Equipment serial number
- CSULA property identification number, if applicable
- The employee to whom it is assigned
- Department name
- Dates checked out
- Classification of information on the device
- If protected data is stored on the device:
  - o Confirmation that the employee has received appropriate training to ensure that the employee will exercise due diligence in safeguarding the mobile computing device and the data it contains.
  - o A copy of the written authorization approving that the storing of protected data on the device is necessary to conduct CSULA business and the acceptance of all associated risks.
  - o A sufficient description of the protected data in case breach notification is required.
  - o The date that the device was replaced or retired and verification that any protected data on the device was disposed of properly.
  - o Signature of the employee and the employee's supervisor.

4.10 Reporting

California Senate Bill 1386 (SB 1386), effective July 2003, modified California Civil Code sections 1798.29, 1798.82, 1798.84 and 1798.85 making 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 Level 1 confidential information. 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 CSULA mobile computing device or their own mobile computing device containing University Level 1 confidential information assume responsibility beyond those of a campus desktop computer user.

Unauthorized physical access tampering, loss or theft of the mobile computing device should be reported immediately to University Police. If the mobile computing device contains Level 1 or Level 2 protected data, a report should be made immediately to the director of IT Security and Compliance. In some cases, a device can be remotely deactivated thus preventing e-mail or other data from being exposed. The Desktop Services Group or department information technology consultant (ITC) should be contacted to remotely deactivate a mobile device (e.g., computer, Blackberry, telephone) if it is lost or stolen thus preventing data from being exposed.

5 Contacts

a) For questions regarding specific department procedures, contact the department administrator.
b) For assistance in reformatting hard drives and other electronic storage media, contact the ITS Help Desk at 3-6170.
c) For assistance with purchasing or using laptop tracking and recovery software, contact the ITS Help Desk at 3-6170.
d) For assistance in encrypting files, contact your department's information technology consultant (ITC).
e) To report a lost or stolen laptop, contact University Police at 323-343-3700, Building 46.
f) To report a security breach, contact the director for IT Security and Compliance at 323-343-2600.
g) Address questions regarding these guidelines to: ITSecurity@calstatela.edu.

6 Applicable Federal and State Laws and Regulations

Federal	Title
Family Educational Rights and Privacy Act (FERPA)	**Family Educational Rights and Privacy Act (FERPA)** http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html A federal law that protects the privacy of student education records.
Gramm-Leach-Bliley Act 15 USC, Subchapter I, Sec. 6801-6809	**Gramm-Leach-Bliley Act** http://www.ftc.gov/privacy/glbact/glbsub1.htm A federal law on the disclosure of nonpublic personal information.

State	Title
California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.85	**California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.85** http://www.leginfo.ca.gov/.html/civ_table_of_contents.html This is a state law that provides information on safeguarding personal information.
SB 1386	**California Personal Information Privacy Act, SB 1386** http://www.info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html This bill modified Civil Code Section 1798.29 to require notification to individuals whose personal information is or is assumed to have been acquired by unauthorized individuals.

7 Related Documents

ID/Control #	Title
CSU Information Security Policy	**The California State University Information Security Policy** http://www.calstate.edu/icsuam/sections/8000/8000.0.shtml This document provides policies governing CSU information assets.
NA	**Property Loan Agreement** http://www.calstatela.edu/univ/materials/proploan.gif The agreement form is required when University equipment is removed from the campus for official University use.
ITS-1005-G	**User Guidelines for Portable Electronic Storage Media** http://www.calstatela.edu/its/policies/ This guideline is intended to help students, faculty, and staff meet the University's accepted standards for protecting confidential information that is copied, downloaded or stored on portable electronic storage media.
ITS-1007-G	**User Guidelines for Laptop Security** http://www.calstatela.edu/its/policies/ This guideline outlines the steps for securing laptops and the personal, confidential or proprietary information contained on them.

ID/Control #	Title
ITS-1008-G	**User Guidelines for Reporting a Lost or Stolen Computer or Electronic Storage Device** http://www.calstatela.edu/its/policies/ This guideline outlines 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.
ITS-1015-G	**User Guidelines for Wireless Access** http://www.calstatela.edu/its/policies/ This guideline helps users meet the University's accepted standards for wireless access.
ITS-1017-G	**User Guidelines for Safe Disposal of Electronic Storage Media** http://www.calstatela.edu/its/policies/ This guideline outlines the steps departments and business units, students, faculty and staff should take to remove data and software and appropriately dispose of electronic equipment/devices.
ITS-1027-G	**User Guidelines for Encryption Security** http://www.calstatela.edu/its/policies This guideline provides information on approved encryption algorithms, recommended encryption products and specific encryption tools and practices.
ITS-2804	**Lost/Stolen Computer/Electronic Storage Device Report** http://www.calstatela.edu/its/forms This form is used to report a lost or stolen computer or electronic storage device to University Police and IT Security and Compliance.
Information Security Tips	**Laptop Security Measures** http://www.calstatela.edu/its/itsecurity/tips/securelaptop.htm This web site provides security measures for a laptop.
Information Security Tips	**Physically Guard Your Laptop** http://www.calstatela.edu/its/itsecurity/tips/phys-laptop.htm This web site offers security tips for physical protection of a laptop.
Information Security Tips	**Safeguard Laptop Contents** http://www.calstatela.edu/its/itsecurity/tips/laptopcontents.htm This web site provides security measures to protect the information stored on a laptop.

ID/Control #	Title
Information Security Tips	**Secure Your Laptop's Wireless Connection** http://www.calstatela.edu/its/itsecurity/tips/securewireless.htm This web site gives information on how to secure a wireless connection for a laptop.
Information Security Tips	**Safeguard Your Laptop When Traveling** http://www.calstatela.edu/its/itsecurity/tips/laptoptravel.htm This web site provides special security precautions when traveling with a laptop.