User Guidelines for Portable Electronic Storage Media	Guidelines No.	ITS-1005-G	Rev:	B
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Acting Director		
	Issued:	3/4/08	Effective:	3/4/08
				Page 1 of 4

1 Purpose

By their very nature, portable electronic storage media require special attention because confidential information that may be stored on them can be easily transported, shared, stolen, or lost. When they are connected to a computer or device on a University network, portable electronic storage media are capable of spreading viruses, worms, and other malware. And, because they are easy to use and relatively small, portable electronic storage media are often used to store music, video, and graphic files. Therefore, students, faculty, and staff must safeguard and secure confidential information stored on portable electronic storage media and to ensure compliance with copyright laws.

These guidelines are 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.

2 Definitions

CDRW Drives and Disks: Compact Disk ReWritable drives and writable optical storage disks that allow users to copy and store data to CDs for backup and archival purposes.

Confidential Information: In addition to the items listed in the Personal Information definition below, confidential information includes, but is not limited to, the following: financial records, student educational records, physical description, home address, home phone number, grades, ethnicity, gender, employment history, performance evaluations, disciplinary action plans, and NCAA standings.

Directory Information: Information about students that the University is authorized to release as governed by the Family Educational Rights and Privacy Act (FERPA).

DVD: Electronic storage media similar in physical appearance to CDs, but that use a different laser (one that allows for more data to be stored on the disk) to read information. DVDs require a special DVD drive. DVD-R is a write-once format. DVD-RW is similar to DVD-R, but has a re-writable format.

Health Insurance Information: 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

Medical Information: Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional

Personal Information: Under California Senate Bill (SB) 1386 and Assembly Bill (AB 1298), personal information is defined as follows:
An individual's first name or first initial and last name in combination with any one or more of the following data elements:

- Social Security number
- Driver's license or California Identification Card number
- Account number, or 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
- Medical information
- Health insurance information

Portable Electronic Storage Media: Includes, but not limited to, the following: CDs, CDRWs, DVDs, Zip disks, flash drives, floppy disks, I-pods, digital media players, and portable hard drives.

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

USB Storage Devices: External portable hard drives that connect to PCs via USB cables, and, after the driver software is installed the first time, are automatically listed by Windows as an available drive. Examples of USB storage devices are flash drives, memory sticks, and pen drives.

Zip Disks: Portable electronic storage media that use a much higher quality magnetic coating than floppy disks, which means that the read/write head on a Zip disk can be significantly smaller than on a floppy disk. The smaller head and use of a variable number of sectors per tracks means that Zip disks can store thousands of tracks per inch on the disk surface.

3 Guidelines

a) All confidential, personal, and proprietary information stored on portable electronic storage media must be encrypted.

b) Users must safeguard their portable electronic storage media from loss and unauthorized access. Lock your portable electronic storage media in a safe place if you leave it unattended.

c) Unauthorized peer-to-peer file sharing of copyrighted works, including music, pictures, movies, and other published materials using University resources is strictly prohibited.

d) The use of any University resource, including campus networks, for downloading or duplicating copyrighted materials such as music files, video, games, and software without the express permission of the copyright holder is strictly prohibited.

e) Portable electronic storage devices connected to any University resource or network must be used for University business, backups of University-related files, and educational purposes only.

f) When procuring portable electronic storage devices, department administrators should ensure that the purchase meets the unit's business plan requirements; the location where the equipment will be kept is secure; and the personnel that will be using the equipment are aware of the state and federal laws, California State University (CSU) executive orders, and Cal State L.A. administrative procedures, policies, and guidelines.

g) CSULA personnel should access and use portable electronic storage media only when there is a University-related business need to do so.

h) University records and reports, regardless of their formats or storage media, must not be removed from campus or the office where they are maintained unless in the performance of job duties and with the department administrator's permission.

i) Backups of mission-critical department business onto portable electronic storage media should be stored in a secure, off-site location designed specifically for records retention and retrieval.

j) Do not transfer information from or to a portable electronic storage device and a computer unless the computer is protected with up-to-date anti-virus software.

k) The movement or disposition of electronic storage media should be done through the Office of Property Management only after the media is completely reformatted by the ITS Baseline Team. If the portable electronic storage media is no longer of use and it is not regulated by the Office of Property Management, it *always* should be reformatted or destroyed by shredding or other appropriate means, but never thrown into a trash container unaltered.

NOTE

If a CD shredder is unavailable, deeply scratching or etching the CDs surface with a sharp object will destroy its readability. For Zip disks and other similar media, the process of reformatting will erase all recorded data on them; however, multiple reformats are necessary to ensure all data is erased. When in doubt about how to dispose of portable electronic storage media, contact the IT Security and Compliance office at extension 323-343-2600.

4 Terms, Conditions, and Sanctions

a) The violation of security precautions for the protection of confidential information may be a crime and may be subject to appropriate legal action and criminal prosecution.

b) Unauthorized peer-to-peer file sharing of copyrighted works, including music, pictures, movies, and other published materials, is a violation of campus computer-use policy. It is also illegal and may carry significant monetary and criminal sanctions. It is the responsibility of students, faculty, and staff who are downloading or uploading files to ensure that these are not copyrighted works, or that the copyright holder's permission has been obtained. Illegal file-sharing and other copyright violations are a violation of Title 5 of the California Code of Regulations.

c) A violation of these guidelines may be subject to disciplinary action, up to and including dismissal, as set forth by statute, including, but not limited to, Education Code section 89535.

d) Users should have no expectation of privacy regarding information that is transmitted over, uploaded to, downloaded from, or stored on University computing resources or systems. The University monitors information on files downloaded over its network.

e) All users of campus computing resources, including those using student labs, must comply with these guidelines.

5 Contacts and Resources

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 in encrypting files, contact your department's Information Technology Consultant (ITC). An ITC locator is online at: http://www.calstatela.edu/academic/aa/ess/itc/.

d) For questions regarding these guidelines or information security, contact IT Security and Compliance at itsecurity@calstatela.edu.

e) Information about FERPA requirements is available online at: http://www.calstatela.edu/ferpa.

f) Links to laws, regulations, statutes, CSU Executive Orders, and campus user guidelines governing the use and handling of confidential information and campus computing resources are available online at: http://www.calstatela.edu/its/policies.

6 Related Documents

ID/Control #	Title
AP 011	**Administrative Procedure: Student Records Administration** Establishes the campus policy and procedure for maintaining student records consistent with Executive Order 796. http://www.calstatela.edu/univ/admfin/toc.htm
ITS-1004-G	**IT Project and Procurement Guidelines** Sets the standards for complying with CSU Executive Order 862. http://www.calstatela.edu/its/policies
University Catalog Appendix F	**Privacy Rights of Students in Education Records** Outlines FERPA requirements concerning educational records and directory information http://catalog.calstatela.edu
ITS-1008-G	**User Guidelines for Reporting a Lost or Stolen Computer or Electronic Storage Device** Procedures for reporting a lost or stolen computer or electronic storage device http://www.calstatela.edu/its/policies