User Guidelines for Securing Offices, Workspaces, and Documents

Guidelines No.	ITS-1006-G	Rev:	E
Owner:	IT Security and Compliance		
Approved by:	Sheryl Okuno, Acting Director		
Issued:	5/21/08	Effective:	5/21/08

1 Purpose

The campus community is responsible for protecting personal, confidential, and proprietary information. Students, faculty, and staff must comply with federal and state laws, California State University (CSU) executive orders, and campus administrative procedures, policies, and guidelines related to information security by taking measures to protect and secure University information. These guidelines are intended to help the campus community protect offices, machines, devices, and documents from unauthorized access to confidential, personal, and proprietary information.

2 Definitions

Confidential Information: In addition to personal information (defined below), examples of confidential information include the following: financial records, student educational records, physical description, home address, home phone number, grades, ethnicity, gender, employment history, performance evaluations, disciplinary action plans, or NCAA standings. Confidential information must be interpreted in combination with all information contained on the computer to determine whether a violation has occurred.

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

Information Security Breach: According to California Senate Bill (SB) 1386: A situation where ". . .unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

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

Metadata: Usually "hidden" information such as the author, company, manager, as well as dates created, accessed, and modified, that is automatically inserted every time a document is saved. Metadata can include manually saved comments, different document versions, memorized undo-redo actions, and edits made by tools (like Microsoft Word Track Changes) that are not deleted until changes are accepted

Personal Information: Under California SB 1386 and Assembly Bill (AB) 1298: 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

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.

Record: "Authentic official copy of a document deposited with a legally designated officer . . . ." (Merriam-Webster Online: http://www.merriam-webster.com/) Records can be in any format (handwritten, printed, digital, etc.) and can be stored on paper, computer media, e-mail, hand-held peripherals, CDs, DVDs, wireless devices, video or audio tapes, films, microfilm, microfiche, or any other media.

Shadow Systems/Confidential Files: Shadow systems and confidential files are any files or applications like third party or home-grown databases, systems, spreadsheets, documents, and tables external to Common Management System (CMS) applications and that contain personal or confidential information. Examples include: Stand-alone payroll or financial systems; student housing systems; library systems; rosters containing student names, addresses, phone numbers, and grades; attendance databases containing emergency contact information; information repositories containing passwords, employee ID numbers, drivers' license numbers, and Social Security numbers; and rosters containing NCAA standings or commuter information.

3 Guidelines

3.1 Securing Offices and Workspaces

a) Lock your office doors and windows whenever you leave your office unattended.

b) Physically secure all laptops, computers, CDs, zip disks, flash drives, and any other electronic storage devices containing confidential information.

c) Ensure that only authorized personnel have, or have access to, office keys.

d) Ensure that only authorized personnel have authority to remove confidential information from the office, and that the information is properly marked "CONFIDENTIAL" and secured for transport.

e) Ensure that department servers are kept in a physically and environmentally secured area accessible only to authorized personnel.

3.1.1 Handling Handwritten or Printed Documents

a) Use a confetti or pulp shredder to dispose of handwritten or printed documents containing confidential or personal information. Do not use a strip-shredder because strips of paper can be reassembled easily.

b) Label all printed reports containing confidential information "CONFIDENTIAL."

c) Label all printed confidential reports that should not be copied "DO NOT COPY."

d) Do not leave documents containing confidential or proprietary information lying on a desk, in an unlocked drawer, in a printer or fax machine, or anywhere that is accessible to unauthorized individuals.

e) Remember to lock file cabinets that contain confidential and other sensitive documents. Do not keep the key in the lock. Secure the key to prevent unauthorized individuals from finding and using it.

f) Retrieve confidential documents immediately after sending them to the printer.

g) Stay at the copier to ensure that all originals and copies of confidential documents are removed promptly when copying is completed.

h) Stay at the fax machine until a confidential document is sent or received in full.

i) Do not delegate tasks related to confidentiality to students or others who are not authorized to work with confidential information.

j) Never leave confidential or sensitive documents unattended. If you must leave your office or workspace, lock all confidential documents in a file cabinet or desk drawer.

3.1.2 Securely Situate Office Workstations

a) Situate workstations that contain confidential records and documents in locked offices or in less traveled, secured areas.

b) Lock your workstation every time you walk away from it. (**Ctrl-Alt-Delete ► Lock Computer**). When returning, press Crtl-Alt-Delete and input your user name and password).

c) Don't walk away from centrally-located workstations if confidential information is visible on the screen. Exit the document or lock your computer.

d) Ensure that your monitor is positioned so that confidential information is not visible to individuals who are not authorized to see it. Consider installing a privacy screen on your monitor.

e) When using transactional terminals, never walk away leaving any transactions visible on the monitor.

3.1.3 Workstations and Electronic Storage Devices

a) Adhere to the *User Guidelines for Portable Electronic Storage Media*.

b) Return workstations to the ITS Baseline Team for reformatting and reimaging prior to disposition or redeployment to other staff or other departments.

c) Store CDs, DVDs, Zip disks, and other electronic storage media containing confidential information in a locked drawer or cabinet or other secured location.

d) 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.

e) 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.

f) 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.

g) Use secured flash drives (memory sticks) to transport information. Use the secured partition of the drive to store encrypted sensitive and confidential information.

h) If a laptop, desktop computer, or electronic storage device is lost or stolen, immediately notify University Police at (323) 343-3700, and submit a Lost or Stolen Computer or

Electronic Storage Device Report. (For more details, see *User Guidelines for Reporting Lost or Stolen or Electronic Storage Device*.)

3.1.4 Department E-Mail Boxes/Voice Mail Boxes

a) Adhere to the *User Guidelines for E-mail and Electronic Communications*.

b) Mailboxes and voice mail that could possibly receive confidential information should be accessed only by those authorized to view and handle that information. Student assistants should not have access to a department mailbox or voice mail if confidential information might be sent to it.

c) Staff employees should never share passwords to e-mail or voice mail accounts with anyone else.

d) The individual responsible for retrieving the contents of a department mailbox or voice mail should have the authority and approval to handle confidential information.

e) When messages in the department mailbox or voice mail are printed or transcribed, follow the steps outlined in Section3.1.1: Handling Handwritten or Printed Documents.

f) Do not forward e-mail or voice mail messages to those who are not authorized to view or hear confidential information.

g) If confidential information is placed in a Public Folder, folder access must be restricted to only those authorized to view its contents.

3.2 Securing Documents

3.2.1 Creating, Publishing, and Distributing Documents

a) Analyze all documents for content and security before you publish or distribute them. Whether writing a report, web page, tutorial, or any other type of document, balance the specific information published with the security risks that information poses to the University, division, department, or business unit. Analyze documents for their content and potential information security leaks so that publishing or distributing them will not be considered a breach of security or confidentiality.

b) Always encrypt electronic documents containing confidential information

c) Proofread your material before publishing it. Ensure that documents for general consumption:

- Do not contain personal, confidential, or sensitive material.
- Do not contain screen captures and other graphics that display personal, confidential, and sensitive information.
- Do not state an actual internal (non-public) server or IP address, but use pseudonyms instead.
- Do not contain University infrastructure design documentation, which is considered confidential information.
- Do not include University project design documentation, specifications, or actual server names. These are considered confidential.

- Have all metadata removed (see section 3.2.2: Removing Metadata from Electronic Documents).

d) Ensure that documents containing confidential information are distributed or forwarded only to those authorized to see that information.

e) Publish electronic documents in formats such as Word, Excel, or PDF that enable security settings to control what readers can and cannot do with the document (i.e., open, print, copy, edit).

f) Web sites and Outlook Public Folders are considered public. Do not post confidential or sensitive information to them.

g) Do not store confidential or sensitive information on a Web server. Keep Web services separate from database services.

h) Access to confidential information via the Internet, Intranet, or Web portals must be authenticated and restricted to only authorized individuals.

3.2.2 Removing Metadata from Electronic Documents

As a final author or the responsible party in a collaboration, do the following to remove metadata from your electronic documents:

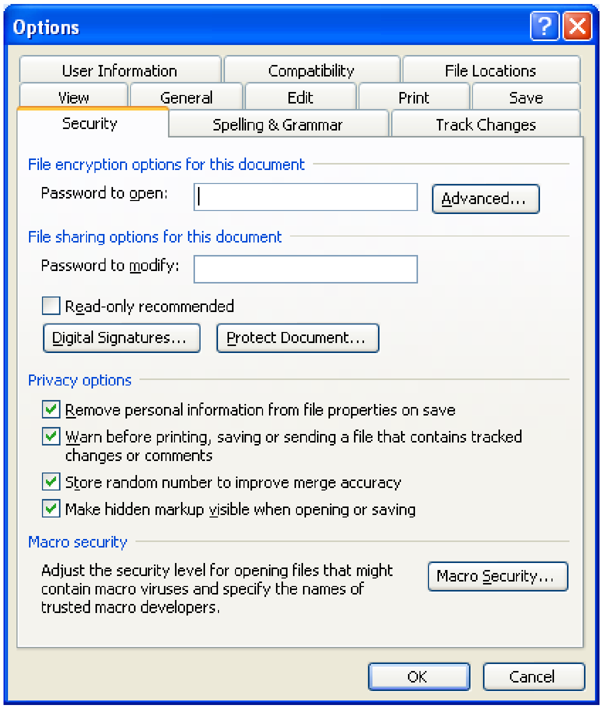
a) Remove all redline edits by accepting all changes. (In Microsoft Word, select **View ► Toolbars ► Reviewing ► ✓ down-arrow ► Accept All Changes in Document**.)

b) Remove all document comments.

c) Use whatever security options exist in an application to delete all metadata when the document is saved, and to warn the author if the document contains tracked changes or comments before printing, saving, or sending the document.

NOTE

In Microsoft Word, select Tools ► Options ► Security tab. Check the boxes under Privacy Options and any other security features desired.



File encryption options for this document

Password to open:

File sharing options for this document

Password to modify:

□ Read-only recommended

Privacy options

☑ Remove personal information from file properties on save

☑ Warn before printing, saving or sending a file that contains tracked changes or comments

☑ Store random number to improve merge accuracy

☑ Make hidden markup visible when opening or saving

Macro security

Adjust the security level for opening files that might contain macro viruses and specify the names of trusted macro developers.

Figure 1. Microsoft Word Options > Security Tab

d) If document “Properties” is available in your application, delete all authors’ and reviewers' names.

e) Disable "fast saves" to ensure deleted information is actually deleted.

f) If document “Versions” is available in your application, delete all previously saved versions in the document.

g) Consider using third party tools to purge or "scrub" your document of all metadata.

h) Remove as much metadata as possible prior to converting your document to PDF format.

3.3 Securing Shadow Systems and Confidential Files

a) Conduct an inventory in your organization to identify shadow systems and files containing confidential, personal, and proprietary information.

b) Rigorously track all files (hardcopy and electronic) that contain confidential information. This includes information on hardcopy reports, CDs, DVDs, and any other media.

c) Ensure that users are authorized to access only those resources required to perform their job duties and nothing more.

d) Regardless of the storage media, ensure that all confidential files at rest and in transit are encrypted to mitigate the risk of unauthorized access.

e) Give a copy of all passwords to the assigned “key master,” someone in a management role who has access to data, in case the file owner forgets them or is unavailable. The key master is responsible for storing the passwords in a secured location.

f) If others need access to an encrypted file, notify them, preferably by phone, with the password to decrypt the file. ***Never e-mail a password***.

g) Rather than e-mailing encrypted confidential data to others on campus, keep it in a separate shared department directory, and allow only authorized individuals to access it.

h) Do not allow reports or files containing confidential information to be handled by student assistants unless they have signed the *Standard Acknowledgement of Confidentiality and Appropriate Use of Accounts for Student Assistants* form.

i) Ensure that all department personnel follow campus and CSU security practices and policies concerning confidential, personal, and proprietary information.

4 Terms, Conditions, and Sanctions

If lost or stolen equipment contains confidential, personal, and proprietary information, the responsibility for notifying victims under SB 1386 and AB 1298 resides with the department or division where the security breach occurred.

5 Contacts and Resources

a) For questions regarding specific department procedures, contact the department administrator.

b) For assistance in reformatting hard drives or other electronic medium, contact the ITS Help Desk at 3-6170, LIB PW Lobby.

c) For questions regarding general information technology security, contact IT Security and Compliance, (323) 343-2600, LIB PW 1070, ITSecurity@calstatela.edu.

d) For assistance in encrypting electronic files containing confidential information, contact your department's Information Technology Consultant (ITC), or contact IT Security and Compliance at (323) 343-2600, ITSecurity@calstatela.edu.

e) For more detailed information on the risks of metadata and ways to ensure content and document security, visit www.metadatarisk.org.

6 Related Documents

ID/Control #	Title
ITS-2804	**Lost or Stolen Computer or Electronic Storage Device Report** Form used to report a lost or stolen computer or electronic storage device http://www.calstatela.edu/its/forms
ITS-8824	**Shared Network Resource Request** Form used to request a shared department directory or other network resources http://www.calstatela.edu/its/forms
ITS-2805	**Shadow Systems/Confidential Files Worksheet** Form used to help individuals inventory their areas for confidential information http://www.calstatela.edu/its/forms
ITS-2803	**Standard Acknowledgement of Confidentiality and Appropriate Use of Accounts for Student Assistants** Form that should be completed by every student or graduate assistant that has access to confidential information http://www.calstatela.edu/its/forms

ID/Control #	Title
ITS-2800	**University Shadow Systems/Confidential Files Vulnerability Assessment** Form used by University employees to report to their deans or divisional vice presidents the shadow systems and files in their areas that contain confidential information and how they are secured http://www.calstatela.edu/its/forms
ITS-1000-G	**User Guidelines for E-mail and Electronic Communications** Guidelines for meeting the University's accepted standards for e-mail and other known or evolving methods of electronic communication or transmission of data and other files http://www.calstatela.edu/its/policies
ITS-1007-G	**User Guidelines for Laptop Security** Guidelines for securing laptops and the personal, confidential, and proprietary information contained on them http://www.calstatela.edu/its/policies
ITS-1005-G	**User Guidelines for Portable Electronic Storage Media** Guidelines to help students, faculty, and staff meet the University's accepted standards for protecting confidential information stored on portable electronic storage media, and for copying or downloading data to them http://www.calstatela.edu/its/policies
ITS-1008-G	**User Guidelines for Reporting Lost or Stolen Computer or Electronic Storage Device** Guidelines that outline the steps users must take when desktop or laptop computers and electronic storage devices are lost or stolen http://www.calstatela.edu/its/policies