



Information Technology Services

Practices for Protecting Electronic Restricted Data: A Quick-Reference
<http://its.ucsc.edu/security/policies/rd.php>

INTRODUCTION:

Because of its very nature, restricted data must be protected from unauthorized access or disclosure. The following practices are designed to provide realistic, achievable steps for protecting this information. *For questions or additional information about any of these practices, please see "Getting Help," below.*

Please note: This document is intended to be a "quick-reference" only. For a more comprehensive list of practices for protecting electronic restricted data, including additional responsibilities for Managers and Service Providers, please see <http://its.ucsc.edu/security/policies/rdpp.php>.


DEFINITIONS:

Restricted Data: The University of California has defined "restricted data" as "any confidential or personal information that is protected by law or policy and that requires the highest level of access control and security protection, whether in storage or in transit."

At UCSC, restricted data includes Personal Identity Information (PII), electronic protected health information (ePHI) protected by Federal HIPAA legislation, credit card data regulated by the Payment Card Industry (PCI), records of students who have requested "Non-Release of Public Information" under the Federal Family Educational Rights and Privacy Act of 1974 (FERPA), information relating to an ongoing criminal investigation, and court-ordered settlement agreements requiring non-disclosure. Please see ITS' online glossary for information about many of these types of data:
<http://its.ucsc.edu/security/policies/glossary.php>

PRACTICES FOR PROTECTING ELECTRONIC RESTRICTED DATA, INCLUDING PII:

1. Securely delete restricted data when there is no longer a business need for its retention. Always shred or otherwise destroy restricted data before disposing of it.
 - i. Information on how to securely delete files is available in IT Request (<https://itrequest.ucsc.edu>):
Mac – FAQ #533; PC – FAQ #822
2. Truncate or de-identify restricted data that you must retain whenever possible.
3. Implement the following protections for all intact restricted data you must retain:
 - i. Be sure that you have **proper authorization** prior to accessing restricted data, and never share or discuss restricted data with unauthorized individuals.
 - ii. Always **store the minimum amount of restricted data necessary** for completing job functions, and remember #1, above.
 - iii. **Use cryptic passwords that can't be easily guessed, and protect your passwords**
 - Good, cryptic passwords use a mixture of upper and lower case letters, numbers, and symbols; are at least 8 characters in length (or longer if they're less complex); are difficult to guess and easy to remember (so you don't have to write them down).
 - Don't share your passwords or private account information.
 - Use different passwords for accounts that provide access to restricted data than for your less-sensitive accounts.
 - For more information, see the *UCSC Password Strength and Security Standards* at <http://its.ucsc.edu/security/policies/password.php>.

- iv. Make sure your computer has all necessary **operating system (OS) and third-party application security updates** or “patches,” as well as **anti-virus**, and that you know what you need to do, if anything, to keep them current.
- v. Ensure proper **physical security** of electronic and physical restricted data.
 - Secure your work area before leaving it unattended.
 - Lock up portable equipment & sensitive material (take keys out of drawers),
 - Lock windows and doors.
 - Never share your access code, card or key, or hold secure doors open for people you don’t know.
 - Physically secure (lock down) workstations whenever possible.
 - Don’t leave sensitive info lying around, including on printers, fax machines, or copiers.
 - Be especially careful with portable electronic devices that store restricted data (such as laptop computers, CDs/floppy disks, memory sticks, PDAs, data phones, etc.). These items are extra vulnerable to theft or loss.
 - Don't keep sensitive information or your only copy of critical data on portable devices unless they are properly protected.
- vi. **Secure laptop computers at all times**; keep it with you or lock it up before you step away, even for a very short time.
 - At all times: in your office, at meetings, conferences, coffee shops, etc.
 - Make sure it is locked to or in something permanent.
 - Take special care with a laptop that includes restricted data; in the event of theft, not only will the laptop be lost, any restricted data on it will be compromised.
 - Laptop lockdown cables are available at the Bay Tree Bookstore and most computer or office supply stores.
- vii. **Be safe on the Internet**: Don't provide personal or sensitive information (including your password) to Internet sites, surveys or forms unless you are using a trusted, secure web page.
 - Look for “https” (not http) in the URL and the little locked padlock  that appears in the corner of most browser windows to indicate that there is a secure connection.
 - Don’t click on unsolicited web links, including in email or pop-ups. Just opening a malicious web page can infect a poorly protected computer, so be aware of where you are going before clicking on a link.
 - Instead of clicking on an unsolicited link, look up web pages you are interested in on your own and go there directly (use a search engine such as Google or Yahoo).
- viii. **Practice safe emailing**:
 - Don't open email attachments or click on website addresses in emails unless you really know what you're opening.
 - Delete spam and suspicious emails; don’t open, forward or reply to them.
 - Email that contains restricted data must be treated with care and should not be preserved any longer than absolutely necessary.
 - Make sure your email client (Thunderbird, Apple Mail, Outlook, etc.) is configured for secure authentication and secure sending and receiving of email. See http://its.ucsc.edu/services/cruzmail/secure_settings/ for configuration information.
 - Configure your email client to delete attachments when emptying the trash. Most email programs have this choice in the preferences, settings, or options.
 - Contact the ITS Support Center (see below) with email questions or problems.
- ix. **Shut down, lock, log off of, or put your computer to sleep before leaving it unattended, and make sure your computer requires a password to start up or wake-up.**
 - **PC**: <ctrl> <alt> <delete> or <Windows><L>
 - **Mac**: Apple menu or power button

- x. **Additional cautions about storing restricted data:**
 - Be sure you know who has access to folders **before** you put restricted data there!
 - Don't put sensitive information in locations that are accessible from the Internet.
 - Don't send or download restricted data to an insecure or unknown computer.
- xi. **Restricted data must be encrypted when it is transmitted.** This includes email, remote access, file transfers, and workstation/server communications.
 - If you send files or attachments containing restricted data, work with ITS to set up a way to send them securely (contact info below).
 - Avoid standard (unencrypted) email and Instant Messaging (IM)
- xii. **Disposal and Re-Use:** Restricted data must be destroyed or completely and securely removed from computers and electronic media (including backups) before disposal, re-use or re-assignment. See #1, above, for links to tools.
- xiii. **Don't use actual restricted data in test or development systems, or for training purposes.** If actual restricted data must be used, it must be protected appropriately.
- xiv. **Don't install unknown or unsolicited programs on your computer.** These can harbor behind-the-scenes computer viruses or open a "back door" giving others access to your computer without your knowledge.
- xv. **Be sure your workstation is set up so that unauthorized people and passers-by cannot see the information on your monitor.**
- xvi. **Immediately report suspected security incidents and breaches** to your supervisor and the ITS Support Center (contact info below). If no one is available, also contact the ITS Security Response Team at security@ucsc.edu.
 - Report lost or missing University computing equipment to your supervisor and the Campus Police (<http://www2.ucsc.edu/police/>), and to the local authorities if the incident occurred away from campus.
- xvii. **Be familiar with UC and UCSC policies relating to restricted data.** Links to many of these policies are available on the ITS Security Awareness website's "Restricted Data Resources" page at http://its.ucsc.edu/security_awareness/restricted_data_resources.php. Also applicable are UCSC's *Acceptable Use Policy* <http://its.ucsc.edu/security/policies/aup.php>, and any specific non-disclosure agreements that apply to information that you work with.
 - See the expanded *General Practices for Protecting Electronic Restricted Data*, items O and P (link below) for additional policy references and information about UC's sanction policies.

GETTING HELP:

For questions or additional information about any of the above practices, please contact the ITS Support Center or your ITS Divisional Liaison:

- ITS Support Center: 459-HELP, help@ucsc.edu, <https://itrequest.ucsc.edu/>, or in-person, M-F 8AM to 5PM, 54 Kerr Hall
- ITS Divisional Liaisons: http://its.ucsc.edu/divisional_liaisons/

ADDITIONAL RESOURCES:

- The ITS Security Awareness website: http://its.ucsc.edu/security_awareness/index.php
- Personal Identity Information (PII) Resources: http://its.ucsc.edu/security_awareness/pii.php
- *UCSC Practices for Protecting Electronic Restricted Data*: <http://its.ucsc.edu/security/policies/rdpp.php>