



Information Technology Services

UCSC Remote Access Guidelines

<http://its.ucsc.edu/security/policies/ra.php>

DOES THIS APPLY TO ME?

The guidelines below are intended to reduce the risk associated with remote access of University information, systems or resources. They apply to people who do any of the following:

- use a computer to work from any non-University location
- connect to campus networks or systems from off-campus, including
 - your workstation
 - campus business systems, such as FIS/BANNER, PPS, AIS, DataWarehouse, InfoView, etc.
 - departmental file systems, shared drives or shared servers
- conduct University business over a non-University network (wired or wireless)
- use a computer for University business that is shared by non-University individuals, including children, family or friends
- use a non-University computer for University business


Managers are responsible for making sure that employees engaging in any of the above activities are authorized to do so and receive appropriate education and training on these guidelines and other applicable UC, UCSC, and departmental policies.

Please note: All individuals with access to UC Santa Cruz electronic information, systems or resources are expected to be familiar and comply with campus policies, practices and guidelines relating to the use and access of these resources. Additional information is available on the ITS Security Awareness web site at http://its.ucsc.edu/security_awareness/. A glossary of terms is available online at <http://its.ucsc.edu/security/policies/glossary.php>.

REMOTE ACCESS GUIDELINES – TO HELP REDUCE THE RISK:

ITS recommends that only University owned and supported computers be used for all remote access activities; however, the guidelines below apply to any computer used for remote access.

For questions or additional information about any of these practices, please see "Getting Help", below.

1. Individuals who need to access their work computer remotely should work with ITS (contact info below) to ensure compliance with applicable policies and security standards for the types of information being accessed.
 - ITS recommends that work computers allowing remote access are managed by ITS to ensure appropriate security.
2. Restricted data should be stored on appropriately protected systems. If you need to put a copy of restricted data on another computer for analysis, store the minimum amount of restricted data necessary and securely delete it as soon as possible (see #5). Truncate, de-identify, or otherwise redact restricted data that you must retain whenever possible.
 - See <http://its.ucsc.edu/security/policies/rd.php> for additional information about restricted data, including definitions and additional practices for protecting it.
3. Passwords and data should be encrypted during transmission to reduce the risk of being intercepted and stolen.
 - Web sites: Web pages that have https (not http) in the web address (URL) encrypt the information you enter. Most web browsers also have a little locked padlock  that appears in the nav bar or a corner of the browser window to indicate that information is being encrypted. Check for these indicators *before* you enter sensitive or personal information, including your

UCSC REMOTE ACCESS GUIDELINES

- password, online. If they're not there, don't log in and don't enter the information.
 - Email: Make sure your email client (Eudora, Apple Mail, Thunderbird, Outlook, etc.) is configured for secure authentication (sign-in). For how to do this with CruzMail, see http://its.ucsc.edu/service_catalog/cruzmail/email_client.php.
 - Don't use the same passwords for University systems as for non-University systems.
4. Email and Instant Messaging (IM) are vulnerable to being intercepted by hackers. If you send or receive email, attachments, files, or IM containing restricted data, work with the ITS (contact info below) to set up a way to do this more securely.
 5. Securely delete or destroy restricted data in email, attachments or other electronic documents when there is no longer a business need to keep it. Also be sure to securely erase or destroy data on computing equipment before disposing of it. For information on how to securely delete files, see: [Mac / PC](#).
 6. Don't let unauthorized individuals access restricted data or protected University systems or applications. This includes making sure that a shared computer does not remember passwords that you have entered. Most programs have a *preferences* or *settings* option that lets you control this.
 7. Make sure a complex password is required for access to your computer, and that you always shut down, lock, log off, or put your computer to sleep before leaving it unattended.
 - If you are using a shared computer, make sure sensitive files or applications are password protected so that others don't have access. See "Getting Help", below, for assistance.
 - See the *UCSC Password Standards* for information about creating complex passwords: <http://its.ucsc.edu/security/policies/password.php>
 8. Physical security is important in a remote work environment.
 - Don't leave sensitive information lying around.
 - Keep laptop computers secure at all times by either keeping them with you or locking them up before you step away, even if for a very short time.
 - Physically secure (lock down) workstations whenever possible. *Note: All workstations containing electronic protected health information (ePHI) must be physically secured.*
 - Lock up portable equipment before you leave an area – especially if it contains restricted data.
 - Be sure your workstation is set up so that passers-by, including family members, can't see sensitive information on your monitor.
 9. When you are using a shared computer, clear web caches, cookies and history and quit the browser and all programs when you are done. This will help clear what you were doing from the computer.
 10. To help protect from hackers and viruses, make sure your computer has all necessary Operating System (OS) and application security updates or "patches," as well as up-to-date anti-virus and anti-spyware.
 11. Don't download or install unknown or unsolicited programs or files, click on links in unsolicited email, or open unexpected email attachments. These can all infect your computer.
 12. If you need to access your work computer remotely, work with ITS (contact info below) to ensure your work computer complies with appropriate policies and security standards. Supervisor approval may also be required.
 13. Portable equipment, such as data sticks/flash drives, CDs, PDAs, phones, etc., containing sensitive data needs to be kept with you or locked up securely when unattended. These items are extra vulnerable to theft and loss. Where feasible, encryption is recommended. Contact the ITS Support Center (contact info below) for recommended tools and software. (Support Center staff: See ITR FAQ 1043)

UCSC REMOTE ACCESS GUIDELINES

14. Immediately report suspected computer security problems, such as an infected computer or possible disclosure of restricted data, to your supervisor and the ITS Support Center (contact info below).
15. Special information for people who work with credit card or health information:
 - If you are connected to the Internet via wireless, you **may not** send/transmit credit card data unless your department has received formal approval from the Campus Controller, and you are using an approved, secure method of transmission.
 - UCSC employees **may not** store electronic protected health information (ePHI) on non-university equipment, even temporarily.
 - Unencrypted ePHI **may not** be stored on portable electronic devices, including laptop computers and portable storage devices, even if they are University owned.
 - Be sure your supervisor knows if your workstation or electronic devices contain or access ePHI.
 - Work with your ITS Divisional Liaison (contact info below) to encrypt all stored ePHI, or to come up with an acceptable alternative under the campus HIPAA policy if encryption is not feasible.

GETTING HELP:

For help with any of these guidelines, contact

- The ITS Support Center at 459-HELP, help@ucsc.edu, http://its.ucsc.edu/support_center/, or in person M-F 8AM-5PM, 54 Kerr Hall, or
- Your ITS Divisional Liaison (DL): http://its.ucsc.edu/divisional_liaisons/index.php.

Please send feedback or questions about these guidelines to the ITS Service Manager for Community and Compliance at itpolicy@ucsc.edu or (831) 459-2779. Thank you.