SECURITY QUICK TIPS

Why protect data? Sensitive data is at risk if your computer is lost, stolen or compromised

- It's your job to keep Cornell's data safe! You may be held accountable for negligent actions or inaction.
- Cornell may suffer significant financial or reputational loss.
- Individuals whose data is compromised could suffer financial loss, identity theft, and unwanted exposure of private information.

What is confidential data?

Data classified as confidential by Cornell policy, state and federal legislation:

- Social Security numbers
- Driver's license numbers
- Credit card numbers
- Bank account numbers
- Protected health information

What are the best practices to protect confidential and sensitive data?

1. Be proactive and keep your computer clean!
    a. Employees should not store confidential university data on their work or home computers or on removable storage devices. In cases where business practices require the use of confidential data, the employee is responsible for contacting tech support for assistance in securing the data (typically through the use of encryption software).
    b. Know data retention policies. No matter the location or level of security, only keep confidential data as long as is necessary.
    c. To help assure that no confidential data is being stored inadvertently, employees should scan their work computer for confidential data regularly.
        i. http://www.it.cornell.edu/services/guides/data_discovery
        ii. Be aware that data scanners may not find all sensitive data particularly in image or encrypted files.
    d. Use Identity Finder's "shred" feature to delete documents and files containing sensitive information.
2. Passwords
    a. NEVER share your netid password.
    b. Do not reuse your password to access other accounts or services.
    c. Change your password regularly- immediately if you suspect it's at risk. http://netid.cornell.edu
    d. Create and remember complex passwords: http://www.it.cornell.edu/security/identity/passwords/strong.cfm
    e. Use password protections to unlock your computer's screensaver and your mobile devices.
    f. Implement a clean desk policy. (No passwords on sticky notes!)
3. Computer Security
    a. Keep your computer software up to date (apply security patches to operating system and third party software. i.e. Windows XP, Mac OSX, Java, Adobe). If regular software patching is performed by your tech support provider, notify them if you notice alerts indicating patches are not being applied.

b. Run antivirus software configured for daily updates and active monitoring.
   Symantec Endpoint Protection – http://www.it.cornell.edu/services/antivirus
c. Don't be fooled! Is it spam/phish or a real Cornell communication?
   i. Phish Bowl (fraudulent email examples):
      http://www.it.cornell.edu/security/safety/phishbowl.cfm
   ii. Verified Cornell communications:
      http://www.it.cornell.edu/security/safety/verified.cfm
d. Connect to the internet securely to access campus services when you are off campus.
   Use Cornell's Virtual Private Network (VPN) – http://www.it.cornell.edu/services/vpn
e. Never email, IM, or text sensitive data. Share documents securely using Cornell's Dropbox.
   http://dropbox.cornell.edu
f. Connect to Internet securely at Cornell. Use RedRover Secure or eduroam.
   http://www.it.cornell.edu/services/redrover/
g. Never access confidential data from an untrusted computer (i.e., a computer you don't own or a public kiosk)!
h. Any confidential data you store should be encrypted. PGP, Office 2010, TrueCrypt.
   http://www.it.cornell.edu/security/depth/practices/data_discovery/encryption/third_party.cfm
i. Use whole disk encryption on laptops that might be used to work with confidential data.
j. Do not regularly login to your computer with an account that has administrative privileges. Instead, use a "restricted" or "user" account for day to day operations.
k. Don't install unauthorized software, including freeware.

4. Physical Security
   a. Use a security cable for your computer in the office and while traveling.
   b. Store mobile devices (any small device that can store data and be stolen easily) out of view when not in use, preferably in a locked drawer or cabinet.
   c. Do not keeping confidential data on mobile devices. They're too easy to steal and less likely to be encrypted.

University Policy and more resources

1. Know and understand the key Cornell Data and IT policies
   a. http://www.it.cornell.edu/policies/university/index.cfm
2. Review the Cornell Security Handbook - *Computer Security at Cornell: Secure Your Computer On and Off Campus*
   a. http://www.it.cornell.edu/security/handbook.cfm
3. IT Support
   a. Contact your local technical support with specific questions.
   b. No support staff? Contact the CIT HelpDesk
      Phone: 607 255-8990
      Visit 119 Computing and Communications Center
      Email helpdesk@cornell.edu
   c. For emergencies, call the Network Operations Center (NOC)
      Phone: 607 255-9900
      The NOC is staffed 24 hours a day, seven days a week.