

# Ten Steps to Safer Computing

Keeping your data safe from various risks--hardware failure, theft, accidents, and prying eyes--is key to protecting the integrity and confidentiality of your information. With 10 simple steps, it's easy to develop good habits that will keep your data safe and secure:

1. Don't store confidential data (SSN, credit card info, DOB) on your computer unless you must. You should never store any confidential or FERPA protected data on a portable device (USB thumb drive, external hard drive, CDs) or personally-owned computer.
2. If storing confidential data on your computer is necessary, delete it securely as soon as you're done with it.
3. Data on your computer should be backed up frequently and the backup should be kept in a secure location, preferable on the network (H: or L: drive).
4. Passwords should be at least 8 characters long, should include letters, numbers, and special symbols, and should be managed carefully.
5. Whenever possible, do not store confidential information on handheld devices (smart phones).
6. If you use a smart phone (iPhone, Blackberry, Droid), be sure to secure it with a password, especially if you access work email on it.
7. Do not send confidential information via email.
8. Take appropriate precautions to avoid viruses, worms, and other attacks on your computer. Keep your updates current.
9. Set a password to wake your computer from sleep or screen saver mode. Do not set your computer to automatically login. Lock your workstation when leaving the office (ctrl-alt-del, Lock Workstation).
10. Take appropriate measures to protect your computer from theft. If you have a laptop, use a security cable during business hours and lock the laptop in a secure cabinet at nights and over the weekend. If your laptop or portable device is lost or stolen, please notify IT immediately.