

KEEPING IT CONFIDENTIAL IN 2007: TIPS FOR PRIVACY & SECURITY OF INFORMATION



ELECTRONIC INFORMATION

- NEVER retain Social Security Numbers (SSN) in a file unless encrypted or truncated to last 4 digits
- NEVER retain any credit card information in an unencrypted file; follow KU policy & PCI standards
- Use a screen saver password & set your screen saver to turn on after 10 minutes of inactivity
- When you leave your seat, "Ctrl-Alt-Delete" to lock your workstation. (Windows key + L works as well)
- Use multiple [Strong Passwords](#)
- Don't share passwords with anyone
- Use secure file servers to store all private information
- Limit storage on your computer's local drive (e.g. "C") to non-essential, non-private information
- Use a secure, encrypted connection when connecting from any off-campus location
- At home, use WPA encryption (e.g. Wi-Fi Protected Access or WPA2) or stronger for wireless networks
- Never use public computing devices when working with any private information—someone may be looking over your shoulder
- Do not think E-mail as private; it is equivalent to a Postcard—anyone can read it along the way
- Use a Firewall
- Install anti-virus software & update it regularly
- Install & run [spyware](#) removal utilities (e.g. weekly)
- Keep your operating system up-to-date & patched
- Back-up your files on a regular schedule (e.g. daily)
- Be careful with email attachments as they may contain viruses
- Don't download software of unknown origin or security from the internet
- Beware of reading HTML formatted e-mail, as malicious code may be embedded in the message
- Change passwords at least every 90 days (Every 45 days is even better)
- If your web browser offers to save your password, always click "NO." Alternatively turn off the password saving feature in your browser.
- Review & purge your electronic files annually, as appropriate
- Follow IT Security Office [Hardening Guidelines](#)
- Know [KU Policies](#) and follow them
- Use a confidentiality statement at the end of all E-mails to notify the recipient of confidential content



PRINTED INFORMATION

- Always keep printed information in a locked, secure area
- Limit access to files/information based on roles (need-to-know)
- Lock doors/cabinets when leaving the office
- Always retrieve copies, faxes, and printouts immediately
- Don't allow faxing of private information (e.g. student records, medical records, credit card info, SSN, etc.) to a public fax machine or publicly located fax unless you are there to receive it
- Re-verify the appropriateness of your transmission & recipient location prior to sending if private information involved (i.e. faxing, mailing, emailing); Ensure you are not transmitting over an unsecured medium
- Recycle paper containing private information only in secure, locked bins
- Always shred or pulverize paper containing personal, private information
- Don't leave your password where it can be seen or easily found. Any passwords written down should be kept under lock & key.
- Review privacy policies for websites you visit & for programs you download or visit, as some may have spyware or tracking mechanisms attached
- Review and purge printed documents annually, as appropriate
- Use a fax coversheet with a confidentiality statement
- Stamp documents "Confidential" & Clean Desk policy



VERBAL INFORMATION

- Don't discuss private or personal information in a public space
- Do not share health or other personal information regarding a co-worker unless you have express permission from that person to do so
- Always be aware of where you are and who may be listening, intentionally or accidentally



PORTABLE DEVICES

- Remember Portable Devices are easy to steal or lose at an airport, bar, restaurant, library, coffeehouse, hotel, etc. –so keep track of your equipment
- Personal Data Assistants (PDAs) should be set to require a password when turned on or inactive for a minute or two
- When you trade, sell or stop using a portable device (e.g. PDA, MP3, cell phone, etc.) reset device to the factory settings & erase the memory (your info will not magically disappear when the device does)
- When using a USB/Flash/Thumb Drives, select a model with security options to protect private information stored on the drive
- Do NOT carry private or sensitive information around on your laptop, PDA, or other device without encrypting the information
- Use VPN/encryption when transmitting from a portable device; you never know who may be "watching"



PERSONAL INFORMATION

- Shred all mail offering credit cards or bank checks if not utilized
- Shred all statements, credit card or otherwise, if you don't retain them in a secure, locked location
- Check your Credit Reports at least annually (See <http://www.annualcreditreport.com> for free information)
- If you suspect credit fraud, contact each of the credit reporting agencies and place a "fraud alert" on your account (See also <http://www.privacy.ku.edu/idtheft>)
- If using social networking sites, use privacy settings to protect personal, identifiable information (MySpace, Facebook, etc.)
- Monitor your tax documents & statements (including W-2s); they often contain SSN and can be removed from an insecure mailbox
- Do not mail checks or credit card information from an unlocked mailbox box; take it to the post office
- Use only one (1) credit card for on-line transactions & carefully monitor statements; check-out "virtual" numbers for on-line, credit-card transactions