

**Washington and Lee University
Guidance on Information Security**

This guidance addresses common issues that have come up during information security discussions with offices and departments across campus. The University encourages all employees to review this guidance and contact Scott Dittman, Information Security Program Committee Chair (sdittman@wlu.edu) or Dean Tallman, Information Security Officer (dtallman@wlu.edu) with any questions involving information security.

1. Be aware of the types of confidential information that you have and only gather/keep what you need to conduct university business.

- The first step to protecting confidential information is to know what you have.
- Confidential Information includes:
 - Social Security, Credit Card, Bank Account, and Driver's License Numbers
 - Financial Asset Information
 - Income and Tax Returns
 - Medical Information
 - Any other information that isn't appropriate for public distribution (including personally identifiable student-record information)
- Consider whether the confidential information is actually necessary, rather than being collected simply out of habit.

2. Take steps to protect hard copies and electronic copies of documents containing confidential information.

- If possible, redact (remove or hide completely) as much of the confidential information as possible. For example, redact all but the last four digits of a Social Security Number if needed for identification purposes.
- If redaction is not possible, store hard copies of confidential information in lockable file cabinets, and keep them locked when not in use.
- Don't store confidential information on computer hard drives, USB drives, laptops, personal computers, personal "cloud" computing resources, or in personal email accounts. Such information should only be stored in the university's approved databases.

3. Remember: email is not secure, even if you are emailing another person at W&L.

- Don't send any confidential information via email, unless you've taken steps to encrypt the contents. Contact Dean Tallman x8089 dtallman@wlu.edu for assistance.

4. Maximize computer security.

- Hit the "Windows" key (on the bottom-left of the keyboard in between the "Ctrl" and "Alt" keys) simultaneously with the "L" key to lock your computer any time you step out of the office. Apple/Macintosh users can lock their computers by using "Apple-L".
- Set up a screen-saver with "password protect on resume" as a back-up measure.
- Use strong passwords. Test the strength of your password at <http://howsecureismypassword.net>.
- Consider the positioning of your monitor, especially if you are in a high-traffic area. If you can't reposition your monitor so as to prevent unauthorized/casual viewing, consider using a monitor privacy screen.

5. Be cautious when providing confidential information to any third party.

- Disclose confidential information on a "need to know" basis only.
- Send any contracts to the Office of General Counsel in advance for inclusion of appropriate confidentiality provisions, particularly where a vendor will need access to confidential information.

6. Take appropriate steps when someone leaves your department.

- Send the person to Human Resources for an exit interview.
- Require the person to return his/her key(s).
- Contact ITS to have the person's network and/or database accesses terminated.
- Ensure that confidential information has been removed from the person's laptop computer and/or other devices.

7. Take appropriate steps to dispose of confidential information.

- All hard-copy documents containing confidential information should be disposed of by secure means only, such as shredding (cross-hatch shredding recommended). Contact Chris Wise (jwise@wlu.edu) if your office would like to participate in the university-wide shredding service.
- All electronic files containing confidential information should be securely deleted through use of a "shredding" program and/or a reformat of the hard drive (as appropriate).