THE UNIVERSITY OF ARIZONA
Information Security

Office Security @ UA

Data security is built on five key principles:

1. **TAKE STOCK.** Know what personal information you have in your files and on your computers.
   - ☐ Inventory computers, laptops, flash drives, CDs – anywhere you and your department stores sensitive data.
   - ☐ Remember that your department receives personal information in a number of ways, so keep this in mind as you perform your inventory.

2. **SCALE DOWN. Keep only what you need for your college or department.**
   - ☐ Use Social Security numbers only for required and lawful purposes.
   - ☐ Shorten or truncate electronically printed credit card information.
   - ☐ Do not keep credit card information unless you have a need for it, and follow the disposal guidelines required by law.
   - ☐ Check default settings on software that reads credit card information or other personal information.

3. **LOCK IT. Protect the information that you keep.**
   - ☐ Store paper documents and portable media in a locked room or locked file cabinet.
   - ☐ Put files away, log off computers, and lock file cabinets and office doors when you are going to be away for your desk or office.
   - ☐ Encrypt confidential and regulated data.
   - ☐ Don't share passwords.

4. **PITCH IT. Properly dispose of what you no longer need.**
   - ☐ Comply with disposal policy guidelines (see **HTTP://RMAA.ARIZONA.EDU**).
   - ☐ Shred paper documents that contain sensitive information.
   - ☐ "Wipe" old computers and portable storage devices of all sensitive information before disposing of them.

5. **Plan Ahead. Create a plan for responding to security incidents.**
   - ☐ All departments should follow the Incident Handling standard (IS-S1100) and guideline (IS-G1100), found at UA Information Security's website.

*** Adapted from the FTC's "Protecting Personal Information: A Guide for Business"*