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.
- ☐ Consider the following:
  - Who sends sensitive personal information to your college or department?
  - How is it received? Email? Through a website? By mail?
  - What kind of information do you collect at each entry point? Consider credit card information and other personal information (i.e., social security numbers).
  - Where do you keep the information you collect?
  - Who has – or could have – access to this information?

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.
- ☐ If you must keep information, follow the retention and disposal policy found on the Records Management and Archives website. As well, the Information Security Office has a flow chart to help you determine if a document is a record you must keep.

3. **Lock It. Protect the information that you keep.**

- ☐ Physical Security
  - Store paper documents, CD, floppy disks, zip drives, tapes, etc. containing personally identifiable or sensitive information in a locked room or locked file cabinet. Limit access to employees with a legitimate business need. Require that these files be kept secure in this

manner. Remind employees not to leave sensitive papers out on their desks when they are not at their workstations.

- 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.
- Implement and follow appropriate access controls to your office and building. If you see suspicious behavior, report it.

☐ Electronic Security

- Identify computers and servers where sensitive information is stored, and use one of the following options to secure this information if it needs to be stored for business purposes:
  - Transfer personal information to a CD, DVD or flash drive and physically secure it
  - Separate the number from the associated name
  - Truncate the number to the last four digits
  - Replace all but the last four digits of the number with filler X's
  - Encrypt personal information

☐ Password Management

- Control access to sensitive information by using "strong" passwords. The longer the password, the better.
- DON'T:
  - Share your password with anyone
  - Post your password near your workstation
  - Keep passwords in a document electronically on your computer
  - Laptop Security
  - Always store your laptop in a secure place when you are not using it, or when it is not in your direct control.
  - Store sensitive information on your laptop. If you must store such information, make sure it is encrypted.

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"*