Tips for Securing Confidential Records

Personal Cubicles & Offices

- **Keep confidential information off of your desk and work area, unless you're working with them, especially in medium to high traffic areas.**
- **Private offices should be locked when unattended and/or all confidential information should be locked in file cabinets &/or in desk drawers.**
- **When meeting with students or guests, remove all confidential information from sight – preferably locked up, in case you need to step away for a moment.**
- **Use small (crosscut) shredders for shredding any notes, photocopies, printouts or other unneeded documents containing confidential information. NEVER THROW CONFIDENTIAL INFORMATION IN TRASH CANS.**

Offices/Departments

- **Use lockable file cabinets or shelving units.**
- **If possible, have a secured folder room with controlled access.**
- **Use an out card system to keep track of folders as they are removed from file cabinets. Include the file name, the date taken and the person taking the file.**
- **The processing section of the office (containing confidential information) should have secure keypad entry for staff & faculty use only. Visitors should only be allowed in the secured area with an escort.**
- **If keypad entry is the main entry into your office, keyed deadbolt locks should be**
- **used after hours or when the office is unattended.**
- **Keep an office shredder (crosscut only) by office copiers and/or shared printers for shredding misprinted copies with confidential information.**

- **For large quantities of confidential documents, microfiche, computer disks, etc., contact a shredding company that provides on-site confidential shredding. (Have a staff member or student assistant, watch the process, making sure all documents are shredded on site.) Locked containers can be left in your office, with prearranged pick-ups with a signed contract with the vendor.**

Basic Tips for Electronic Records Security

- **Do not place confidential information on the subject line of an email.**
- **Place privacy screens on computer monitors to avoid easy viewing by others.**
- **Use password protection on all computers.**
- **Confidential information should be stored on university network servers, never on personal hard drives or computer desktops.**
- **All computer equipment should be locked down.**

Link to "Tips from the IT Security Awareness Team"
Visit http://www2.gsu.edu/~wwwsec/ for more detailed information on computer security awareness.