Sensitive Data on Copiers, Scanners, Printers and Fax Machines
Susan Blair, UF Chief Privacy Officer
Kathy Bergsma, UF Information Security Manager

PRIVACY RISKSPOSED BY COPIERS: The Information Privacy World took another step forward recently as CBS broke a story about how common copiers used across all businesses contain “hard drives” that retain images of everything copied by that copier. There are hundreds of copiers in use throughout the University of Florida containing hard drives that retain images of every document that the copier has copied. This poses a serious risk that anyone who may come into possession of a copier used at UF that comes off lease, or is discarded and then refurbished or resold. Identity thieves or others may pull sensitive information off the hard drive from that copier and misuse that information.

In addition, scanners, printers and fax machines may also have an installed memory chip or hard drive that retains images of printed, copied or faxed documents. So, all of your basic office equipment potentially poses a risk.

DUTY TO SECURE COPIERS, SCANNERS, PRINTERS and FAX MACHINES: As a result, the University must take precautions to ensure that copiers, scanners, printers and fax machines are protected and do not pose a risk that any information retained by that machine is inappropriately used or accessed by an unauthorized person.

Every UF department is responsible for ensuring that all copiers, scanners, fax machines and printers are properly secured from the point of delivery to the time of disposal.

WHAT YOU CAN DO TO SECURE YOUR OFFICE EQUIPMENT. UF employees in each department must assume responsibility for securing the copiers, scanners, fax machines and printers in their department and must take one or more of the following actions:

1. CONTRACTS FOR COPIERS: One important step you can take is to ensure all new contracts or purchase orders for copiers include a contractual clause (or language in the purchase order) that requires the vendor/service provider to provide one of the following:

   a. Include an encryption solution or other secure data solution on your copier that encrypts or overwrites the hard drive on the copier; or

   b. Securely erase the data on the hard drive or securely destroy it upon removal for service or return to the vendor at the expiration of the lease. The service provider should be required to produce a signed ‘certificate of destruction’ that includes the model number and serial number of the hard drive, before taking the copier’s hard drive off the premises. When you are ready to return the copier to the vendor, you’ll place a service call with the copier service vendor, and request a secure data erase or removal of the hard drive (see below). You’ll then obtain a signed certificate of destruction with the hard drive model and serial number. The vendor will need to show you the hard drive

drive and verify the serial number and model number so that when they provide you with the certificate, it will match the hard drive you gave them.

c. Your other option is to include language in your contract/P.O. that requires that the vendor offer you the hard drive for purchase at the end of the lease. In this case, you’ll ask for the vendor to send a technician at the end of the lease to come and remove the hard drive so that you may submit it to your IT department for secure destruction.

In each of these instances, whether you purchase some sort of data security encryption product or ask for a secure data wipe, or the return of the hard drive, you will incur an additional cost. So, you will need to remain active in your efforts to determine what solution works best in your particular environment.

2. PURCHASING ENCRYPTION OR SECURE DATA SOLUTIONS FOR YOUR COPIER. Many copier companies are aware of issues with hard drives on their copiers and already have a number of security solutions in place. As mentioned above, you can purchase an encryption solution for the copier’s hard drive or an overwrite program that overwrites data onto the hard drive effectively rendering the images unreadable. These solutions can often be installed on both new copiers upon delivery, or on existing copiers already in use. Again, you’ll simply need to place a call to your copier vendor to ask what sort of solutions they offer to protect the data on the copier you own/lease or are about to lease or purchase.

3. PRINTERS, SCANNERS AND FAX MACHINES. This same problem may also exist with printers, fax machines and scanners as well. Talk with your supplier about whether or not the model you use stores information, and if so, the same actions should be performed before disposal of fax machines and scanners. You may have to ask your IT Department to remove any memory device in your printer, fax machine or scanner prior to disposal.

HOW THE UF JACKSONVILLE CAMPUS SECURED THEIR COPIERS AND OTHER EQUIPMENT. In Jacksonville, the UF Jacksonville campus purchasing department worked with the Privacy Office and Contracts Office to identify the most appropriate solution for this problem. They started by meeting with their copier vendor to discuss their options. Their solution involved having the vendor install a disc overwrite system on their 125+ copiers already in use. For all new copiers, the vendor agreed to include the disc overwrite system on each new copier delivered to the campus. Additionally, all departments are being advised to contact the IS Department prior to the disposal of any printer, copier, scanner, fax machine or other multifunction device. That way, if there is a hard drive in the machine, it will be disposed of in a secure manner.

Your solution should start with an inventory of the office equipment in your department or area, and then expand to discussions with your copier vendor(s) for options available to you. It’s important that you take the first steps to open the dialogue with your copier vendor as your copier vendor will likely have a number of possible solutions for you to consider. Since printers,
scanners and fax machines aren’t typically leased or returned to the vendor, your review should focus on a secure method for disposal of these machines.

Below are a number of helpful web sites, some of which are referenced above, that may help you understand your obligation to protect the sensitive data on copiers, printers, scanners, and fax machines. If you have any questions about securing your copier or if you have any questions about information contained in this communication, you can send an e-mail with your question(s) to security@ufl.edu.