

Security Concerns with Copiers, Printers and Multi Function Devices (MFD)

In response to some inquiries and comments from some University departments on the publication done by CBS titled "[Digital Photocopiers Loaded With Secrets](#)", Document Services & Solutions (DSS) explains:

- The University identified this risk sometime ago, thus we are not as exposed as stated in this news article.
- The Information Technology Security team addressed this risk three years ago and they performed an audit of the Ricoh fleet. Based on IT's recommendation Ricoh encrypted their hard drive with proprietary software, and we asked IT Security to verify and audit our devices. IT Security performed forensics and discovered that the drives were indeed utilizing a proprietary format and were unable to read any information on them.
- Ricoh performs a routine, at installations/removals, which has been built into its systems that erases all customer programmed, customer stored and customer sent data. Ricoh technician formats the entire content of the hard drive and all information stored on the machine is effectively gone.
- IT Security conducts random audits to make certain Ricoh is in compliance. Additionally, IT Security regularly audits using the latest audit techniques to recommend additional security measures as needed.

If you have any additional concerns please contact DSS at 305-284-2378 or at DSS@miami.edu

DSS-May 13, 2010