Copier and MFD Security

Eight Steps to Secure Your Copier or Multi-Function Device (MFD)

✓ *Note:* The resources below have been gathered to specifically address concerns related to the security of sensitive information that may be stored on the hard drives of copiers, printers, or multi-function devices. However, it is good practice to develop a general minimum security standard for ALL networked devices. Issues related to media disposal, confidential data handling, patching, encryption, third-party contracts, etc. are not unique to the devices mentioned here.

1. **Configure copiers, printers, and other multi-function devices securely.**
    - Configure the device with a static IP address, using RFC1918 (non-routable) addressing if possible.
    - Limit network access to the device, by configuring IP restrictions (firewall or ACL) for the device to only those needed.
    - Change default admin password to a strong value, and change community string names.
    - Disable all unneeded services, protocols, and features. Often just TCPIP is needed, and ports 9100 (HP Jet Direct) and/or 515 (LPD).
    - Employ a method to erase or overwrite the hard disk between jobs, such as setting a job timeout value.
    - Refer to the following university resources below: Brown, Indiana University, Northwestern, UC Davis, UC Irvine, UT Austin, and Yale.
2. **Develop appropriate policies and procedures that address disposal procedures for equipment, protecting sensitive data, etc.**
    - Always employ appropriate disposal procedures for equipment. *When in doubt, consult the manufacturer for proper sanitization procedures.*
        - Destroy/shred/erase internal hard drives before decommissioning
        - Negotiate contract terms that include secure wiping/disposal for leased equipment
    - Refer to the following university resources below: Indiana, University at Buffalo, and University of Florida.
    - This HEISC resource includes a survey of higher education disposal policies and practices: Guidelines for Information Media Sanitization.
3. **Work with vendors to make sure devices meet industry security standards and certifications.**
    - Be sure to review current contracts. If security concerns arise, work with vendors to close the gaps and modify/update contracts as needed.
    - Develop a template for contact/service agreements with vendors that have devices with more native security features. Many vendors also offer optional data security kits.
    - Refer to the following university resources below: Brown, Indiana, UC Davis, and UC Irvine.
4. **Educate IT staff, business offices, and other users on campus.**
    - For IT support, make them aware of university policy and practices, especially regarding proper disposal of electronic equipment, and any contracts or special fees that are required for equipment.
    - For faculty/staff/students, alert them to the risk of making copies off-site coupled with information about the institution's policy and practices. It's also a good opportunity to tie in a more general reminder about PII and the reasons to protect it.
    - Refer to the following university resources below: Brown and University of Florida.
5. **Remember to perform firmware updates on a regular basis. Upgrades are often a manual process.**
    - Some vendors offer security updates via RSS Feed (e.g., Xerox).
    - Refer to the following university resources below: UC Irvine, UT Austin, and Yale.
6. **Consider managing all copiers/multi-function network devices through one office, and utilize print spool servers.**
    - With a central print spool/queue service, you can limit direct printer access to only that server.
    - Refer to the following university resources below: Boston University, Broward College, and University of Akron.
7. **Consider requiring drive encryption.**
    - Refer to the following university resources below: UC Irvine.
8. **Consider physical security of hard drives for devices with open access.**
    - Remind faculty/staff/students to avoid copying documents with sensitive information using public-access devices.
    - Post flyers or label machines in public places as a reminder that any data copied there may be stored in the memory.
    - Move printers or copiers to more secure (and less open) spaces whenever possible. Consider housing them in an area that is staffed, and locked after hours.

Additional Resources for Copier & Multifunction Device (MFD) Security

Higher Education Resources

- Boston University: Printing Services
- Broward College: Document Output Management Strategic Planning
- Brown University: Security Standard for Multi-Function Network Devices
- Brown University: Secure IT! Newsletter - What's On Your Copier?
- Florida State University: Auditing Security Controls of Printers, Scanners, and Multifunction Devices (2010 Presentation)
- Indiana University: Protecting Data in Copiers and Multifunction Devices
- Northwestern University: Guide to Securing Networked Printers, Scanners, Copiers, and Faxes
- University at Buffalo: Secure Wiping of Print Device HD's
- University of California, Davis: Data Privacy with Multi-function Printers, Printers and Copiers
- University of California, Irvine: Printer and Copier Security Best Practices
- University of Florida: Media reuse and disposal standard, Copier and Multi-Function Device Safeguards
- University of Tennessee: Multi Function Device Best Practices
- University of Texas at Austin: Multifunction Device Hardening Checklist
- Yale University: Multifunction Printer Security and Compliance & Multifunctional Device (MFD) Hardening Standards
- HEISC Guidelines for Information Media Sanitization

Industry & Other Resources

- ACM: Multi-Function Device Security Awareness
- Bruce Schneier: Printer Security
- Canon USA: Product Security Information

- CBS News: Copy Machines, a Security Risk?
- CIO.com: How to Reduce the Risk of Insecure Firmware in Office Gear
- CIS: Security Benchmark for Multi-Function Devices
- Computerworld: Smart Printers, Scary Printers - The Surprising Security Threat: Your Printers
- Congressman Markey: Announcement about FTC Investigation into Privacy Risks of Digital Copiers, Letter to the FTC, and FTC Response to Congressman Markey
- DISA: Multi-Function Device (MFD) and Printer Checklist for Sharing Peripherals Across the Network - Security Technical Implementation Guide
- ENISA: Secure Printing
- FTC Bureau of Consumer Protection: Copier Data Security: A Guide for Businesses
- GCN: NIST Outlines Guidance for Security of Copiers, Scanners
- HP Secure Erase for Imaging and Printing
- NIST IR 8023: Risk Management for Replication Devices
- NIST SP 800-88: Guidelines for Media Sanitization (see appendix A for copy & fax machine sanitization recommendations)
- PC Magazine: How to Securely Dispose of a Printer
- SANS Institute: Auditing and Securing Multifunction Devices
- SANS Internet Storm Center Diary: Digital Copy Machines - Security Risk?
- SecurityFocus: Canon Remote UI Reveals Usernames and Passwords in Address Book
- TechRepublic: The Truth About Copier Hard Drives: Tips for Securing Your Data
- Xerox: Security Bulletins

Questions or comments? Contact us.