

Copier and Multi-Function Device

Management Procedure to Improve Security, Service, and Reduce Related Costs

Background

Copiers and multi-function devices (MFDs) have become more affordable and convenient. However, these devices may present a security risk because some contain a hard drive or similar storage to make the device more efficient and the service convenient. Additionally, environmental and financial concerns require consolidation of individual office printers and copiers whenever possible and that the most cost effective option is selected (for example a leased MFD or the service available from SCSU Printing Services). There are resources available to you on our campus that can assist with the selection of such devices. This procedure is designed to assist you with the management of MFDs in your department.

Purchasing or leasing new copier/scanner/fax/printer or multi-function device (MFD)

When beginning the search for new copier, scanner, fax, printer, or a combination MFD, ensure that you contact the following areas for advice:

- Printing Services (savings are likely with anticipated use of over 10,000 copies per month)
- Your technician or the campus Computer Store
- Business Services

Printing services may offer competitive options for specialized printing needs and especially for high-volume printing.

The technician and the Computer Store will be able to recommend supported models and the most cost effective models that meet your department's needs. Consolidation of printers and MFDs should be considered whenever possible to reduce costs and impact on the environment. While a small printer for an individual office may seem inexpensive, there are usually substantial costs of maintenance and toner.

Business Services will provide information on cost effective leasing options available to SCSU departments.

You should work with these departments before contacting vendors directly so that you receive unbiased advice for the most cost effective option.

Managing existing equipment

- If the equipment is 3 years or older, inquire about a replacement (see the Purchasing section above). Among other disadvantages, old equipment draws a substantial amount of energy even when not in use.
- Work with your technician to determine whether the device has a hard drive. If one is present, it should be encrypted and the device should be secured with a PIN or a password.
- Additionally, work with your technician to determine if the device has a "disable storage" option.
- If the device has storage enabled and it cannot be turned off, determine who will purge the stored information and how frequently that will be done.
- Work with your technician to ensure that any MFDs on the network are secured (guide attached).
- Physically secure equipment so that access is controlled.
- Ask for identification of any outside parties requesting to service the printer. Ensure that your technician is present in case the hard drive is removed or replaced.
- Beware of "social engineering" calls from unknown parties that ask for the model of your copier or MFD. There are vendors that try to sell overpriced substandard supplies.

Returning equipment at end of lease

Per State of Minnesota contract requirement, leasing vendors must scrub data on MFD hard drives and provide SCSU with a certificate attesting to that fact.

The department's technician must attempt to scrub any stored data if possible. A scrubbing utility is available for HP devices. Leasing vendors may return the hard drive to the department before accepting the unit at disposal. In that case the hard drive must be physically damaged to the point where it will not be possible to read the data from it.

Transferring old equipment

Because the MFD equipment is likely to contain sensitive data after being used, the department should contact the computer technician to scrub the data. The device should not be released to the outside vendor or another department or State entity until the data has been scrubbed or the internal storage device physically destroyed. If the storage device is not easily accessible, the equipment should be disposed of through an authorized vendor. Please contact the Inventory unit of Business Services for additional information

Disposing of or retiring old equipment

When disposing of purchased equipment, the department should contact the computer technician to scrub the data. After that the Inventory unit of Business Services must be contacted so that the device is picked up and securely stored before being passed to a contracted vendor for disposal. Additional information on equipment disposal is available at http://www.finance.mnscu.edu/contracts-purchasing/collaborative/docs/disposition_general_summary1.pdf

Outside printing, copying, and other document services

Occasionally a department may choose to use an outside printing or copying service (such as FedEx Office). This approach is often not cost effective and SCSU Printing Services should be consulted first. Additionally, caution should be exercised when using such vendors as there is no assurance that the equipment used is set up in a secure manner. It is possible for sensitive data to be retained and exposed by using such services. Copyright laws must be respected to ensure that protected works are copied only when permitted and only by individuals allowed to do so.

Guide for Technicians

1. Enable PIN numbers or passwords if available. All users should have individual passwords to access the device if possible.
2. Review vendor documentation for any listing of security related features and enable as appropriate.
3. Turn off MFD hard drive storage if practical.
4. If a hard drive is required, it should be encrypted.
5. Establish a strong administrator password on the device.
6. If the hard drive is replaced, ensure that the old hard drive is scrubbed or destroyed (see resources below).
Leasing vendors must provide certificate of data destruction if they retain the hard drive. If the storage is inaccessible, ensure that the device is disposed of through an authorized vendor through the Inventory unit of Business Services.
7. Monitor work done on the device by outside technicians.
8. For networked devices, consider consulting with IT to determine if the device should be placed onto a Virtual LAN for networking communications isolation. (Devices that print reports from the Uniface system may not be placed onto a Virtual LAN)
9. Where the device supports access control lists (ACL), configure them to block all traffic, except for those devices that must communicate with the MFD.
10. Turn off SNMP, FTP, Telnet, Appletalk, Netware and any other unneeded protocols or services.
11. Ensure that patches and updates are regularly applied to the device.

12. Use https to manage the device if available.

Links to additional information on MFD security and scrubbing instructions (where available):

- Xerox Devices: <http://www.xerox.com/information-security/product-security/enus.html>
- Ricoh Devices: <http://www.ricoh.com/about/security/product/index.html>
- HP Devices: <http://www.hp.com/large/solutions/hp-disk-erase-white-paper.pdf>
- Lexmark Multi-function Printer security features:
http://www1.lexmark.com/documents/en_us/CIP_Piece_POD.pdf
- Canon imageRUNNER Devices: <http://www.usa.canon.com/gmd/pdf/HDD-Encryption-and-Overwrite-Brochure.pdf>