Multi-Function Devices/Printers

Effective Date: [08/01/2010]
Last Revised: [08/01/2010]

Audience

All Staff

Policy

Since MFD's use hard drives to fulfill their tasks, the IS Department should be notified whenever a MFD is attached to any network. Each MFD will have an IP address set up and assigned to it by IS. Documents being "scanned to send" should only be sent to moody.edu email accounts. For data security reasons these devices should not be utilized to store confidential and sensitive data or to bypass local network firewalls. All files, folders and other saved data should be password protected and removed by the user as soon as the business process has been completed. The Procurement Department will act as the MFD site administrator. Concurrent with all Moody IT practices all passwords should be changed every six months, including administrative passwords. All future MFD installations will be set up with a sixty day programmed Scheduled Image Overwrite. During off-site service repairs and when end of life cycle occurs, Moody will take active measures to purge and securely sanitize all MFD hard drives.

Definitions

MFD's are any office machine which stores image data on the device's internal hard drive and incorporates the functionality of multiple devices such as: printer, copier, scanner, fax and e-mail that have network capabilities.

Procedures: n/a

Documents

Consult contractual agreements with all known providers of services and equipment suppliers.

Contacts

If you have questions or concerns about the execution of this policy, you may contact the Information Systems Help Desk at x4001 or ishelp@moody.edu for assistance.

If you have questions about the policy, you may email ispolicy@moody.edu for assistance.

Related: n/a