Digital Copier Scanner Device

**Policy Id:**
IT.017 - Digital Copier Scanner Device

**Contact:**
Joseph Laub, Interim Chief Information Officer (212) 484-1108, jlaub@jjay.cuny.edu

**Last Modified:**
January 1, 2013
Policy or Procedure Description:
IT.017 is the City University of New York notice to the CUNY Community for Digital Copier, Scanner security risks and recommended actions.

NOTICE TO THE CUNY COMMUNITY
DIGITAL COPIER, SCANNER SECURITY RISKS
Document type: Advisory
The City University of New York
University Information Security Office, security.cuny.edu
Status: Published, June 2010, Version 0.4 (June 21, 2010), draft for discussion

Many state-of-the-market multi-functional (e.g., copiers, scanners, facsimile functions, printers) digital output devices retain information on an internal hard drive(s) as part of executing these functions. For example, when several copies of a document are needed, the document is scanned once and the copies are made from the file that has been saved on the internal hard drive. Additional examples of when data may be saved on the internal hard drive include printing from a local area network or faxing/scanning a document from the device to an e-mail address. With a hard drive and data which may reside upon them, these devices are similar to a desktop computer that is attached to a network.

Through the normal course of conducting College and University business, documents containing non-public University data (e.g., social security numbers, financial aid applications/reports and student grade information) may be scanned, duplicated, e-mailed, and faxed with residual images retained on the hard drive. When these devices are in need of repair and/or replacement the internal hard drive with data, unless erased and/or disposed of properly, could be extracted and used inappropriately creating potential risks to the University for breaching private information.

The following practices should be adhered to in using, operating and maintaining multi-functional digital output devices:
- Device maintenance engineers must be supervised at all times.
- The immediate copier area should be cleared of all documents that may contain non-public University data. For a definition of non-public University data please refer to the IT Security Procedures at security.cuny.edu.
- Removal of equipment for replacement, removal or disposal must be approved in writing by the University custodian of the equipment.
- Prior to copier removal or disposal the hard drive will be overwritten to accepted industry security standards (e.g., at least three times overwrite) or physically removed and destroyed.

The University will continue to work with our copier vendors to ensure the following administrative and technical criteria are met and maintained throughout the life cycle of the equipment from installation to decommissioning and disposal.
All copier maintenance agreements will be reviewed and approved by the Office of General Counsel and the University Information Security Office. A maintenance agreement if part of a New York State Office of General Services contract may be supplemented if the following requirements are not met:

- A vendor non-disclosure agreement.
- The hard drive in the copier must be locked into position within the device which can only be removed by an authorized maintenance engineer.

- The device must be configured to allow the residual storage of documents only for the time it takes to complete the requested function and then automatically deletes and overwrites the data to accepted industry security standards (e.g., at least three times overwrite).
- Residual storage of data on the hard drive must be protected by a complex password and data encrypted to accepted industry security standards (e.g., 128 bit AES) transparently managed by the copier device.
- Upon replacement, donation or retirement of devices, the hard drive will be overwritten to accepted industry security standards (e.g., at least three times overwrite) or physically removed and destroyed prior to the copier leaving University property.

Our constituents are reminded that compliance with the Policy on Acceptable Use of Computer Resources and the IT Security Procedures is required at all times.