



KONICA MINOLTA

Kevin Kern

Senior Vice President, Marketing
Konica Minolta Business Solutions U.S.A., Inc.

Date: April 26, 2010

Subject: Digital MFP Security

A recent CBS News broadcast raised the issue of security of hard drive data in digital multifunctional products. Konica Minolta would like to assure you that we are a leader in the area of MFP security. Our MFPs can ensure documents that are copied, scanned, faxed or otherwise transmitted, do not remain stored on the hard drive or in DRAM memory as a standard feature. Additional standard security capabilities include:

- **ISO 15408 EAL Level 3 Certification for the Total System Architecture**
Konica Minolta MFPs are independently certified to the ISO 15408 Data security standard as established by the Common Criteria for Information Technology Security Evaluation. While some vendors may only certify a component of the MFP or a "security kit," the entire system architecture on Konica Minolta MFPs is certified.
- **Password Protection**
The built-in hard drive of the MFP is protected by a 20 digit alphanumeric password. This password is stored in the hard drive BIOS and prevents access to the hard drive data, as long as the correct password has not been entered. Therefore, even the removal of the hard drive and installation into a PC, laptop or other MFP would not allow access to the hard drive.
- **Hard Drive Encryption**
128 bit AES encryption for any data temporarily stored on the hard drive. This includes scanned documents and other data.
- **Hard Drive Reformat**
At disposal a key operator, administrator or technician can physically format (erase) the hard drive if the MFP needs to be relocated or at the end of lease. The hard drives can be overwritten (sanitized) using up to eight different highly secure methods including DOD, NASA, Air Force, and NSA standards.
- **Data Auto Deletion**
Data Auto Deletion allows an administrator to set an auto deletion timer for data stored in the personal or public user boxes, as well as system boxes (e.g. secure print box or encrypted PDF print box). The auto deletion setting will erase the copy, print, scan or fax jobs stored in boxes, depending on the storage period and the time frame selected for deletion. The data is automatically erased using a highly secure, U.S. Department of Defense (DoD), overwrite method.

Konica Minolta is committed to supporting your IT security requirements. We not only conform to current internationally recognized data security standards, but sit on the committees that are developing future information technology security standards. We also offer a wide range of security solutions and services beyond the standard features of our products including integration into corporate IT security and authentication systems and Common Access Card support for DOD and government applications.

For more details on our range of security capabilities and offerings, [click here](#) to visit our Security Webpage or feel free to contact your authorized Konica Minolta representative.

Sincerely,

The essentials of imaging