



KONICA MINOLTA

## **Konica Minolta Business Solutions U.S.A., Inc. MFP Security FAQs**

Konica Minolta has been a leader in the area of MFP security for many years. Our products contain some of the most comprehensive security features in the industry. More importantly, we have offered these security features as standard items on most of our MFP products delivered in the past five years.

While Konica Minolta provides a broad range of standard security tools and options, ***it is the customer's responsibility*** to ensure that their use of the product conforms to their IT security protocol. Similar to, Servers, Laptops and other network appliances that contain a hard drive, most office MFP products must be treated as an IT device at both the installation and disposition of the product. Another important consideration is that a vast majority of equipment in our business is leased through third party leasing companies and Konica Minolta has no control over the devices at the end of contract as they are the leasing companies' asset.

The following information is provided to help you answer questions you may have regarding Konica Minolta MFP hard drive security.

### ***1. In light of the recent CBS new feature regarding digital copiers and hard drive risks – How can I ensure that copies of print, scan, fax or copy jobs are not stored unknowingly on the bizhub hard drive?***

The CBS story misrepresented a key fact. Most MFP devices do not store all copy print scan and fax data. Konica Minolta MFPs do NOT store any data or images from standard print, scan, fax or copy jobs as a standard feature. Only if the customer chooses to use functions like the box feature or secure print, can documents be stored on the MFP hard drive.

### ***2. If it doesn't use the Hard Drive, how does the MFP process copy, print, scan or fax jobs?***

For most of our monochrome office line, the hard drive has been, and still is an option. These devices can copy, fax, print and scan documents even if the hard drive is *not* installed.

#### ***2A. How?***

It's similar to a PC where most of the time the document is processed in Random Access Memory(RAM) which is deleted as the pages are processed

#### ***2B. What happens to the job after it is processed in the MFP's memory?***

Once the job is processed, printed or transmitted, it is purged from memory once the next job is received or after the device is turned off. It is physically impossible to extract the job from the machine after the job is processed.

**3. What about the models that contain a hard drive, like color MFPs? Can document image data ever touch the hard drive?**

Again, like your PC, if the device is processing many jobs concurrently some of the image data may spill over onto the hard drive for temporary processing. Once the job is completed, the bizhub MFP can be set to automatically overwrite any residual data that is left over on the hard drive. This is a *standard* function that is built into Konica Minolta's products.

**4. Is automatic hard drive overwrite of temporary data the default setting in the device?**

No, although the default setting is off; our end user documentation and training materials, suggest that this should be turned ON upon installation. We also have standard SLA's with many of our customers that contain this requirement.

**5. We have seen that the Hard Drive in the MFP can be used to store electronic documents. What types of jobs might be stored on the bizhub MFP's hard drive?**

If enabled, electronic documents are stored in the device hard drive into what's known as electronic mailboxes. Think of these boxes as electronic folders on the hard drive.

Konica Minolta calls this the "BOX" function. This function is enabled by some of our most security minded customers.

**5A. What types of BOX functions are there?**

Types of BOX functions include:

- Scan to Box
- Public
- Private
- Print to Box
- Public
- Private
- Secure Print Box
- Incoming fax jobs routed to a BOX

These functions have to be enabled by the end-users MFP Administrators.

**6A. In light of the recent CBS News feature... why would some of your "most security minded customers" be using the BOX function.**

Because they see the obvious benefits of converting paper to digital files using the bizhub MFP's scanning functionality, and they do not want to enable scan to email or scan to a network repository. This technology allows users to scan to a private, password protected, secure BOX for later retrieval.

Our customers configure their bizhub MFP to overwrite (*to U.S. Department of Defense specifications*) any documents residing in ANY Box after a certain period of time. Some security minded customers set the time before automatic deletion of a file in a BOX down to as little as 30 minutes.

These customers also enable hard drive encryption. As with our hard drive overwrite methods, the encryption algorithm uses the stringent Advanced Encryption Standard (AES) standard, which meets US Government and military requirements.

**7. Why would some customers not allow scan to email or scan to a network repository?**

Because scan to email might stretch network bandwidth. Additionally IT administrators do not want the extra burden to administer these functions on the MFP. Scan to BOX function is perceived as less work and in some cases more secure than scanning to Email or scan to a shared folder on the network.

A related question...

**7A. The CBS News feature warns against storing documents on the MFP's hard drive. What does Konica Minolta provide to protect data stored inside the Hard Drive's electronic "BOX"?**

Since 2005, Konica Minolta has provided several standard "out of the box" functions protecting data that could reside in the MFP's hard drive:

- Automatic Job Overwrite (Temporary Data Overwrite)
- HDD Lock Password
- Automatic Deletion of Jobs Stored in an electronic USER BOX
- HDD Overwrite (HDD Sanitizing)

These Hard Drive data protection functions can provide assurance that what was depicted in the CBS story cannot happen to an owner of a bizhub MFP provided they use the features we have in the product.

**7B. Can you explain what these functions are?**

Detailed explanations can be found in our Security White Papers, Vulnerability Statements and Security manuals found on our public web site.

**8. What about end of lease or end of life of the machine? How can I be assured that any image data is completely removed and cannot be recovered by sophisticated data extraction software?**

As detailed in our User Security Guides, Security White Papers and Training Materials,, bizhub MFPs support what is known as hard drive sanitization or hard drive "wipe". *This function is standard, and built into Konica Minolta MFP.* We give the end-user up to 8 choices of hard drive sanitization, conforming to various military and international overwrite standards. The simple process involves pressing 4 buttons on the MFP's control panel... it takes about 30 seconds to initiate the procedure.

**9. What about older machines that do not contain the built in hard drive sanitize function?**

The customer has several choices here.

- We can remove the hard drive and hand it over to the customer's IT department who has standard processes in place to wipe the drive using standard "off the shelf" software applications. After this process is complete the sanitized hard drive is and then installed back into the machine.
- Konica Minolta can remove the hard drive, hand over it to the customer who then may opt to physically destroy the device. In the event the leasing company requires that the MFP is returned with the Hard Drive... Konica Minolta has a program in place to replace the old hard drive with a new clean drive before returning it to the leasing company. The customer will be charged a labor fee and the cost of the new drive.

**10. What about devices that I have returned in the past?**

If they don't contain a hard drive there is no exposure.

If they contain a hard drive and employees didn't use the electronic mailbox application... there is very little risk.

**10A. What about those devices where we used the mailbox function?**

Most of the Konica Minolta MFPs in the marketplace stored data in the mailbox in a proprietary format for our customer's protection that is difficult to access by external means. A person would have to remove the hard drive, have expertise and be deliberately looking for data.

Konica Minolta realizes that protecting electronic documents processed by bizhub MFPs is an absolute requirement in the 21st century workplace. Our customers can count on Konica Minolta to deliver the highest level of security in our award-winning product lines.

This material is copyrighted by Konica Minolta Business Solutions U.S.A., Inc. and is the sole property of Konica Minolta Business Solutions U.S.A., Inc. Duplication of this proprietary report or excerpts from this report, in any manner, whether printed or electronic (including and not limited to, copying, faxing, scanning or use on a fax-back system), is illegal and strictly forbidden without written permission from Konica Minolta Business Solutions U.S.A., Inc. Violators will be prosecuted to the fullest extent of the law.

**Konica Minolta Business Solutions U.S.A., Inc.**

100 Williams Drive

Ramsey, NJ 07446

[www.CountOnKonicaMinolta.com](http://www.CountOnKonicaMinolta.com)