XEROX® Date: 4/10/2007

Subject: Volatility statement for the WorkCentre 4150 multifunction printer

The WorkCentre 4150 does not retain any latent user image in the mechanical system of the printer during normal operation. If a print job is disrupted prior to completion a latent image may exist in the mechanical systems of the printer; cycling power or printing a page will remove the image.

The WorkCentre 4150 does not retain any latent image in the print controller (raster image processor) or associated RAM following the completion of printing. No user data is maintained in the print controller or associated RAM following the cycling of power.

The WorkCentre 4150 contains non-volatile flash memory contained on the controller. This memory does not retain any variable printing data, but can be used to retain software updates, store fonts, etc. No user information is retained in this memory.

The WorkCentre 4150 hard disk drive will retain latent images in the hard disk only when the job retention features are enabled / utilized (Secure print, sample print, or saved print or job accounting) or for scanning.

A procedure for securely erasing any hard disk data can be located in the Customer User Manual

The WorkCentre 4150 contains non-volatile memory in the form of an MSOK (Master System Operation Key). This key does not retain any variable printing data, but does retain printer configuration details, configuration details, printer serial number. This key can be removed and/or destroyed to eliminate the stored data.

The WorkCentre 4150 contains non-volatile memory in the form of customer disposable PEK's (Product Enablement Key). These serve only to enable specific device features and can only be used once. The PEK does not store any device information.

Memory types for the WorkCentre 4150 are:

Model Number	**Memory Size Standard/ Maximum**	**Memory Type**	**Volatility**	**User Data**
4150/C	256MB	SDRAM	Volatile	Yes
4150/S	256/384 MB	SDRAM	Volatile	Yes
4150/X	256/384 MB	SDRAM	Volatile	Yes
4150/XF	256/384 MB	SDRAM	Volatile	Yes
4150/S/X/XF	40GB	Hard Disk	Non-volatile	Yes
All models	16MB FAX receive	SDRAM	Non-Volatile for a minimum of 100 minutes after power off.	No

Internal Hard Disk File Security

Xerox MFP Models

1. Supported Printers

Xerox WC4150 Multi Function Printer models now incorporate security features for data stored on the printer's internal hard disk.

2. Types of data stored on the printer's internal hard disk

An internal hard disk is a standard feature for WC4150S/F/XF models.

The internal hard disk on a MFP is used in several ways to improve printing performance, to implement additional features, and to improve printer usability and management. Security-conscious users often wish to know what types of data are stored on the internal hard disk.

When present, the printer uses the internal hard disk for the following purposes and data types:

a. The printer stores page content data for **Saved**, **Secure**, **Sample**, and printer-collated print jobs. Print jobs sent for immediate printing, e.g. **Normal** jobs that do not use printer-based collation do not have their page content data saved on the printer's internal hard disk.

   For **Saved**, **Secure**, **Sample**, and printer-collated print jobs, the printer must be able to access each page in a print job out of the order they were transmitted to the printer, and possibly at a later time. Because the contents of only a few pages at a time can be stored in RAM memory, the page content data is stored on the printer's internal hard disk. These types of print jobs are not available without an internal hard disk.

   Page content data files are stored in a proprietary, unpublished compressed binary data format. These data files are not directly accessible from any printer interface other than the standard controls or commands for printing jobs, e.g. no feature exists for transferring or retrieving this data to another computer or printer.

   For **Proof**, **Secure**, and printer-collated print jobs, the printer deletes the page content data files when the print job is completed.

   Print job page data files may pose a data security risk because they contain the images of the pages in the print job.

b. The printer can store print job resources, such as fonts, macros, and forms on the internal hard disk. Printing performance is improved when common resources used across multiple print jobs are stored on the disk instead of contained within every print job data stream that uses those resources.

These types of resources must be explicitly copied to the printer's internal hard disk by a user by using a printer utility program, such as the Xerox Font Management Utility. Other utility programs exist from Xerox and other vendors for managing resources of various types on a printer's internal hard disk.

PostScript and PCL fonts may be listed and deleted from the printer's internal hard disk through the FMU.

Print job resource data such as fonts are not likely to pose a data security risk. Customer designed PostScript forms or PCL Macros may or may not pose a data security risk depending on their contents. In any case, storing these types of resources on the printer's internal hard disk is entirely at the user's discretion. The printer never creates such disk files without a specific command to do so by a utility program.

c. The printer records job accounting and usage profile information on the hard disk. Xerox MFP's that support

networking maintain a history of jobs printed, with the details of each print job such as user name, job name and the number of pages. This job accounting data can be viewed from the printer's internal web server, or downloaded to a host computer.

Small amounts of job accounting data are stored in printer NVM flash memory.

The job accounting record data is stored in printer NVM flash memory.

Job accounting data may be deleted from the printer through the printer's internal CentreWare IS web server.

Job accounting record data may pose a data security risk because the names of users, as well as the titles, date, time and lengths of printed jobs can be exposed. The contents of print job pages are not stored in the job accounting system.

3. Secure File Overwrite

When a file is deleted or removed by most computer operating systems, the actual data contained in the file remains on the hard disk mechanism after the command to delete the file is completed. Only the directory entry for the file is deleted and the file no longer appears through the typical operating system software interfaces that access the hard disk.

The areas on the hard disk that stored the deleted file's data are marked as free and available for reuse, and may over time be overwritten by other data as other files are created and written to the hard disk. The deleted file's data, however, is still present for an unpredictable amount of time after the file is deleted. Depending on the amount of hard disk activity, this data may remain on the hard disk for a considerable period of time.

By using special software and techniques, it is sometimes possible to read the data of a deleted file from a hard disk, if it has not been overwritten by the data of other files. This creates the possibility that an unauthorized person with the proper technical knowledge could recover data from a sensitive file, even though the file has been deleted.

On Xerox MFP's, the format of stored print jobs on the printer's disk is in a proprietary, unpublished binary format. While this would prevent casual interpretation of the data, a person with sufficient technical skills would probably be able to reverse-engineer the structure and format of these files and interpret the data.

To address these security concerns, Xerox MFP's now support a Hard Drive Overwrite Security software feature. This feature obliterates the data stored on the hard disk of a file marked for deletion, before the file's directory entry is removed and its storage space on the hard disk is marked as available for reuse.

The obliteration of the data is accomplished by overwriting the entire area of the hard disk that stores the data of the file to be deleted with a pattern of all 'zero' bits, then all 'one' bits, then with a random pattern of bits.

This technique is described in the United States government industrial security standard DoD 5200.28-M. This standard can be viewed at: https://rimr.tatrc.org/DoD1.html . Xerox MFP's that support Hard Drive Overwrite Security fully comply with this standard.

The Hard Drive Overwrite Security feature is not enabled by default. It can be enabled from the printer's front panel.

The following requirements apply to overwriting all images that are stored in spooling areas of all disks.

On Demand Image Overwrite Algorithm

PATTERN: the size of each pattern shall be one byte. The system shall support any characters from the ISO 8859 –1 (UTF-8) character set to be contained within a pattern.

ALGORITHM: The algorithm for disk scrubbing shall be as follows:

Step 1: the binary value of Pattern #1 shall be written to the entire spooling areas of all disks

Step 2: the binary value of Pattern #2 (or the Complement of Pattern #1) shall be written to the entire spooling areas of all disks.

Step #3: the binary value of Pattern #3 shall be written to the entire spooling areas of all disks.

Example:
Value for Pattern #1: The ASCII character "5"
Value for Pattern #2: the complement of Pattern #1
Value for Pattern #3: The ASCII character "ú""

When Hard Drive Overwrite Security is enabled, all files deleted from the printer's internal hard disk will be overwritten, regardless of the printer software controls or commands that deleted it or what type of file it is. There are no exceptions to this rule.

4. Automatic File Deletion (Held Job Timeout)

The printer's administrator can configure the printer to automatically delete any job including unprinted **Secure**, and **Sample** print jobs after a specific amount of time has elapsed since the job was sent to the printer. The time range is from 1 minute to 120 hours.

This option is set from within the printer's Local UI behind a SA only pass code.

Files deleted with Automatic File Deletion are subject to Hard Drive Overwrite Security if that feature has been enabled.

5. Immediate Image Overwrite

The printer's administrator can configure the printer to automatically overwrite any print job including unprinted **Secure**, and **Sample** print jobs after the job has successfully completed printing.

This option is set from within the printer's Local UI behind a SA only pass code.