

# Certificate of Volatility

Manufacturer: **Xerox**

Equipment Name: **WorkCentre / WorkCentre Pro**

Model: **232, 238, 245, 255, 265, 275**

Configuration: This item is networked to print servers with operating system Unix or Windows 2000 or Windows 2003

General description: **This printer is connected to a network.**

Purpose: **Multi-Functional Device, Copy, Print, Analog Fax, Internet Fax, Network Fax, E-mail, and Network Scanning functions. Note that Analog Fax, Internet Fax, Network Fax, E-mail, and Network Scanning functions are optional.**

## 1. **Type of memory:**

**Volatile memory:** What is the amount? What period of time does the unit need to be powered off to completely erase this memory?

### **User Interface Volatile memory:**

**DRAM:** 8 MB (No user image data stored.)

### **Scanner Volatile Memory:**

**SRAM:** 128 KB (No user image data stored.)

### **Copy Controller Volatile Memory:**

**EPC DRAM** 64 MB to 512 MB (User image data stored. Data overwritten after each job so no long term retention)

**SRAM** 16 MB (Setup and User image data stored.)

### **FAX Card Volatile Memory:**

**SDRAM** 64 MB (No user image data stored.)

### **Network Controller Volatile Memory:**

**DRAM** 128 or 256 MB (System and User image data stored. Data lost at power off.)

### **Video Volatile Memory:**

There are also a number of RAM buffers in the video path that are used for image manipulation (Reduce/Enlarge, etc.), and all have no data retention capability. When power is removed all data is lost. These buffers are typically built into the ASICs. Typical bleed down time for all volatile memory is 10 seconds.

# Certificate of Volatility

## Non-Volatile Memory:

**Type:** What type(s) of non-volatile memory are included, EPROM, EEPROM, Flash memory, NVRAM, and battery backed, etc. (fill in)

### User Interface Non-Volatile memory:

Flash ROM: 4 MB (UI executable code. No user image data stored.)

### Scanner Volatile Non-Volatile Memory:

DADF ROM: 1 MB (Scanner executable code. No user image data stored.)

### Copy Controller Non-Volatile Memory:

Flash ROM 8 MB (OS and Copy Controller Control executable code. No user image data stored.)

NVRAM 32 KB / 128 KB (Xerographic setpoints. No user image data stored.)

### FAX Card Non-Volatile Memory:

Flash ROM 4 MB (FAX executable code. No user image data stored.)

Flash NVRAM 32 MB to 256 MB (User FAX image data stored.)

### Network Controller Non-Volatile Memory:

Boot PROM 512 KB (Boot code. No user image data stored.)

NVRAM 32 KB (Configuration code. No user image data stored.)

Rigid Disk Drive: 80 GB (OS, PDL Interpreters, fonts, MIB Objects, Network Protocols, Document Scheduler, and User image data stored. User data overwritten if optional image overwrite option present and enabled.)

There are other non volatile memory devices in the multi-functional device, but these are used solely for low-level I/O control. Some examples of this distributed control are:

- Power distribution, Photoreceptor and main drive motors control
- Raster Output Scanner (ROS)
- Paper Registration
- Finisher

2. **Accessibility:** Is it accessible by accidental/intentional keystroke, or software malfunction?  
**No.** However, the login system administrator or service technician (via diagnostic operation) may adjust certain machine operational parameters. User data is never accessible.
3. If "YES, it **is** accessible, describe location and purpose.

Purpose: typical uses for non-volatile memory location are system identification number and system configuration, boot, and initialization parameters, for example (battery-backed NVRAM on SUNs); put in for future design needs, internal depot repair, clock circuit, "nice" to have, or to flag unauthorized software, etc.

If "NO", it is not accessible, \_\_\_\_\_**X**\_\_\_\_\_ (Check here).

4. *Required memory:* Is device needed for normal operation, i.e. required for this processing period?

## Certificate of Volatility

All memory listed is required for normal operation.

5. *Removal consequences:* If device memory chip is erased, what impact will this have on operation and normal function of device?

Example: If the SUN is turned on without this means of checking for the authorized configuration, the system will not boot and therefore the data cannot be processed per the standard Practice Procedure (SPP).

ROM memory device content is required and essential for operation and normal function of the device. Loss would render the device inoperable.

ROM memory, as stated above, never contains user data. This memory is never overwritten or erased during normal operation.

EPC DRAM memory processes user data. Content of this memory is lost at power off.

Network Controller Rigid Disk Drive removal will result in a message being posted to the local user interface that the disk is not present, and machines ability to handle complex network scanning, E-mail, Internet Fax and Network Fax jobs will be affected. This disk contains customer document images only; no system software is ever present. All customer data is completely overwritten using a 3-pass methodology by the Image Overwrite Security option.

6. *Method of access:* How is it accessed? Is non-volatile memory location theoretically accessible with any system code, not just via the operating system or low level booting firmware?

There is no user access to the memory devices, except as provided programmatically to control device behaviors.

Remember: Modifying internal programming to access is not the same thing as unknowingly accessing from an accidental keyboard stroke.

7. *Warranty:* Does chip removal or EEPROM erasure void the warranty?

Yes, memory removal or erasure will void the warranty. Disk removal of the internal disk drive will void the warranty.

8. *Size:* How much memory is contained? Number of bytes, etc.

See section 1, "Type of Memory"

9. *Spacing:* Is the memory fully utilized or does it have available memory space for additional information to be placed?

The non-volatile memory devices are sized to contain the necessary amount of data required for system operation. Usually there are some unused memory addresses where additional information could be theoretically stored. Without access to the software developers' memory maps, determining the location of this unused memory would require reverse engineering the software.

The Network Controller rigid disk drive contains a 4GB spooling partitions designated for customer document data. Space is dynamically allocated to each job handled; at job completion this space is deallocated to be available for new document images. All residual customer data in deallocated space is overwritten using a three pass algorithm by the Image Overwrite Security option.

## Certificate of Volatility

10. Can this non-volatile memory be addressed to ensure that only authorized information is resident? If yes, how?  
*At boot-up, the system computes a checksum for each non-volatile memory device. (Note: The computed checksum is compared against a value stored in the device itself. This is sufficient to detect hardware failures, but not necessarily intentional corruption.)*

Evaluation and summary of this equipment was completed by the following:

*R. Cusick* Signature

Randall R. Cusick (Printed name)

Technical Marketing Manager (Title)

Product Security Program Manager (Job function)