June 2010 V1.1

Internal Hard Drive File Security

For Phaser Printer Models

45xx
55xx
6250/63xx,
7300/7400/7500
7750/7760
84xx/85xx/85xx MFP

For additional information or clarification on any of the product information given here, contact Xerox Support.

Disclaimer

The information provided in this Xerox document is provided "as is" without warranty of any kind. Xerox Corporation disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Xerox Corporation be liable for any damages whatsoever resulting from user's use or disregard of the information provided in this Xerox Product Response including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Xerox Corporation has been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential damages so the foregoing limitation may not apply.

Table of Contents

Introduction

This document is written to allow security-conscious users to gain some understanding and learn some best practices for use of Xerox Phaser products. The document details which security features are present on Phaser printers. Further security information can be found at the Security@Xerox web site

Supported Printers

Xerox Phaser printer models incorporate security features for data stored on the printer's internal hard disk. Refer to the printer's documentation or visit http://www.xerox.com/officeprinting to determine if a particular model of Phaser printer supports internal hard disk security options.

Some earlier models of Xerox Phaser printers cannot be upgraded to support internal hard disk security.

The information in this document applies to the following Phaser models.
45xx
55xx
6250/63xx,
7300/7400/7500
7750/7760
84xx/85xx/85xx MFP

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

An internal hard disk is an optional feature for some models of Xerox Phaser printers. Not all printer models can support an internal hard disk. The internal hard disk on a Phaser printer 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:

Saved Job Data

The printer stores page content data for **Saved**, **Secure**, **Proof**, 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.
Saved, **Secure**, **Proof**, 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 Xerox 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 page content data files are deleted by the printer when the print job is completed. The page content data files for **Saved** print jobs are stored on the printer's internal hard disk and accessed through the printer's CentreWare IS internal web server or the printer's front panel, until they are explicitly deleted by the user. Print job page data files may pose a data security risk because they contain the images of the pages in the print job.

Job Resources

The printer can store print job resources, such as fonts, macros, color tables, 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 built-in CentreWare IS web server.

Print job resource data such as fonts, and color tables 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.

Job Accounting Data

The printer records job accounting and usage profile information on the hard disk. Xerox Phaser printers 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 and amount of ink or toner used. 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 RAM memory when an internal hard disk is not present, usually the most recent 50 to 500 print jobs depending on available RAM. Job accounting data in RAM memory are lost when the printer is powered off or restarted. When an internal hard disk option is present, the printer stores much more job accounting data, usually 5000 records. This data is also preserved across printer power off or reset cycles.

The job accounting record data is stored in a Xerox proprietary, unpublished binary data format on the internal hard disk. 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.

Added Data Available

Additional features are available through the printer's internal CentreWare IS web server when an internal hard disk option is present. Examples include user manuals in PDF format, QuickTime instructional videos on printer operation and user maintenance, and downloadable printer drivers. This content is preloaded onto the hard disk by Xerox. This additional content data is invariant over time, and does not pose a security risk. No user controls or commands exist for modifying or deleting these additional content data files.

PDF Direct Printing

Some Xerox Phaser models support PDF-Direct printing. For those models that support this feature, an internal hard disk is required for the feature to operate. The PDF document format requires non-sequential access to the file's data. Since a PDF document may be too large to fit entirely in printer RAM memory, the PDF file is first stored on the printer's internal hard disk before it is processed.

Print jobs sent to the printer using the PDF-Direct page description language may pose a data security risk because the print job data stream is written to a temporary file on the printer's internal hard disk. The temporary file is deleted when the print job is completed.

Printer Neighborhood

Xerox Phaser printers support a "**Printer Neighborhood**" feature in the printer's CentreWare IS internal web server. This feature performs a network discovery to find other Xerox Phaser printers on the network, and can optionally discover non-Xerox printers as well.

To increase the performance of this feature, the printer stores the list of discovered network printers in a cache file on the internal hard disk, if it is present. The printer discovery data cache is stored in a Xerox proprietary, unpublished binary data format on the internal hard disk.

The printer discovery data cache may pose a security risk because it contains a network address listing of additional printers. There exists no user controls or commands to delete this cache file once it has been created. The "**Printer Neighborhood**" feature is disabled by default. Do not enable this feature to avoid creating this cache file.

File Creation on the Hard Drive

Files can be created on, modified, and deleted from the printer's internal hard disk through standard PostScript or PJL/PCL file and resource commands. Normal printing jobs from the standard Xerox print drivers do not create these types of PostScript or PCL files.

Specialized printing application software, or custom software or PostScript programs created by a user may create and store files on the printer's internal hard disk. Such data files created by the user may or may not pose a data security risk based on their contents; but the creation and installation of these files on the printer's disk are entirely at the user's discretion.

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 Phaser printers, the format of stored print jobs, discovered network printers, and job accounting data 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 Phaser printers 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.

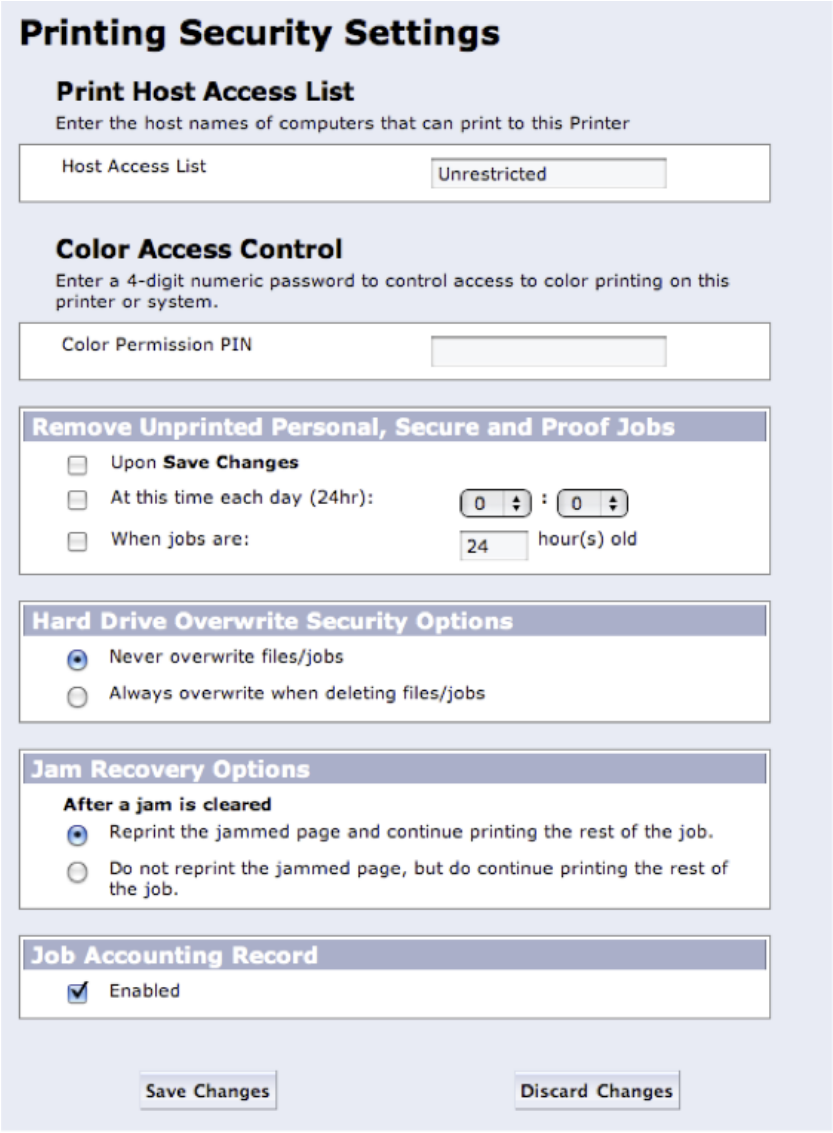
Xerox Phaser printers that support Hard Drive Overwrite Security fully comply with this standard. The Hard Drive Overwrite Security feature is not enabled by default. It can be enabled from the printer's front panel or from within the printer's CentreWare IS internal web server; see section 5 of this document for details on configuring security features. When the Hard Drive Overwrite Security option is enabled, the system command to delete files in the printer's operating system moves the files to be deleted from the printer's internal hard disk into a special directory, where they are processed by a background task on the printer. This background task performs the Hard Drive Overwrite Security process as described above, and then deletes the file directory entry. This software design, by using a temporary folder, insures that the Hard Drive Overwrite Security process will take place for every file, even if the printer is restarted while the Hard Drive Overwrite Security is processing files. 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.

Automatic File Deletion

The printer's administrator can configure the printer to automatically delete unprinted **Secure**, and **Proof** print jobs after a specific amount of time has elapsed since the job was sent to the printer; or after at certain time of day, or immediately upon pressing a button. These options are set from within the printer's CentreWare IS internal web server. Files deleted with Automatic File Deletion are subject to Hard Drive Overwrite Security if that feature has been enabled.

Setting Printer Security Features

The printing security settings of the printer, including security settings affecting files on the printer's internal hard disk, can be configured from within the printer's CentreWare IS internal web server, from the "Security" selection available in "Properties" tab. See the following screen capture (from a 6360 with IPv6 update, other products will be similar but may differ slightly in options available) for the relevant section of Centreware IS. Under the Hard Drive Security Options, select "Always Overwrite When Deleting File/Jobs".



Additionally the same function can be performed from the Control Panel under the Printer Setup File Security menu.3>